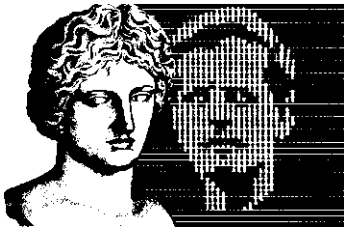
21e rapport d'activité 2000

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Édition 2001



La documentation Française

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

21e rapport d'activité 2000

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

ISBN 2-11-004861-1

Sommaire

« Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

Tel est l'article 7 de la Charte des droits fondamentaux qui a été proclamée solennellement à l'occasion du Conseil européen de Nice le 7 décembre 2000.

On ne saurait trouver, 23 ans après l'adoption de la loi française « informatique et libertés », meilleure consécration de la protection des données personnelles et de la vie privée. Encore ce mouvement ne se borne-t-il pas à l'Union européenne. Ainsi, l'Argentine vient de se doter d'une loi spécifique quand le Canada et l'Australie ont étendu l'application de leur législation protectrice, jusqu'alors cantonnée au seul secteur public, aux activités marchandes. Le gouvernement sud-africain a lancé un livre vert sur le commerce électronique qui comporte un chapitre sur la protection des consommateurs et la vie privée ; le Japon poursuit ses travaux préparatoires d'une législation qui fixerait des principes de base devant être complétés par la déontologie. Quant aux États-Unis, l'effet conjugué des accords conclus avec la Commission européenne sous le nom de « safe-harbor » et des exigences des associations de consommateurs explique sans doute que près de 300 propositions de lois soient déposées dans les Etats et une douzaine au niveau fédéral dans le souci d'assurer enfin une protection à l'égard du traitement informatique des données.

C'est sans doute l'un des effets les plus heureux de ce qu'il est convenu d'appeler la « marchandisation » des données personnelles : en ce domaine,

démentant les prévisions les plus pessimistes, la globalisation pourrait contribuer à l'universalisation de la protection, inventée par l'Europe il y a maintenant plus de 20 ans.

Et la France ? Ici ou là (ici surtout I) on regrette que d'importants chantiers législatifs n'aient pu aboutir aussi rapidement qu'espéré. Il y a urgence désormais à transposer en droit interne la directive européenne du 24 octobre 1995 et à adapter sur plusieurs points la loi « informatique et libertés ». Il convient sans doute aussi, puisque désormais les esprits y sont prêts, à décliner les principes qui sont les nôtres, c'est-à-dire les principes français et européens, au moment de légiférer sur « la société de l'information ». Sur ces deux sujets, et à la place qui est la sienne, la CNIL qui a été consultée par le Gouvernement a fait part de ses réflexions d'ensemble et des orientations qu'elle aimerait voir suivies. Ses travaux sont publiés dans le présent rapport.

Mais l'attentisme, moins encore l'attentisme désolé ou chagrin, ne saurait être la marque de l'institution.

Aussi la CNIL, qui a vu cette année ses moyens renforcés, a-t-elle entrepris une réorganisation de ses services en créant une division des affaires européennes, internationales et de la prospective, une véritable direction de l'expertise et des contrôles qui comportera un service spécialisé en charge des missions d'investigations sur place et en réorganisant sa direction juridique autour de deux « pôles » mieux identifiés : une division des affaires publiques et sociales d'une part, une division des affaires économiques d'autre part. Au sein de cette dernière division, le « pôle » « Réseaux, Télécommunications, Net-économie » sera renforcé et un secteur « Relais-entreprises », guichet unique des PME, sera créé. Enfin, l'augmentation du nombre de plaintes et de réclamations conduit à mettre en place un véritable service de renseignements téléphoniques à la disposition des particuliers. Cette réorganisation qui anticipe la mise en œuvre de la future loi devrait permettre à la Commission d'accomplir ses missions dans de meilleures conditions au service de l'ensemble de ses interlocuteurs : administrations, collectivités locales, entreprises, particuliers.

Enfin, la présentation de ce rapport d'activité ne serait pas complète si l'on taisait les efforts importants que la Commission déploie depuis de nombreux mois pour la réussite de son prochain grand rendez-vous : la XXIII^{e} conférence internationale des commissaires à la protection des données qui aura lieu à Paris du 24 au 26 septembre 2001. « Vie privée : droit de l'Homme », tel sera notre drapeau.

Michel GENTOT

Chapitre 1

LA CNIL EN 2000

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, 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'Etat.

Bilan 1995 -2000

Nature des saisines	1995	1996	1997	1998	1999	2000	Variation 1999/2000
Demandes de droit d'accès indirect	243	320	385	401	671	**817**	+ 21,75%
Plaintes	1 636	2 028	**2** 348	2 671	3 508	**3 399**	-3,107%
Demandes de conseil	985	1 008	821	1 115	1 061	**1 049**	-1,13%
Demandes de radiation des fichiers commerciaux	263	277	263	204	186	**144**	- 22,58 %
Demandes d'information générale	365	347	480	477	396	**319**	- 19,44 %
Demandes d'extraits du fichier des fichiers	122	170	155	154	133	**208**	+ 56,39 %
Total	**3 614**	**4 150**	**4 452**	**5 022**	**5 955**	**5 936**	- 0,32 %

Les demandes d'exercice du droit d'accès indirect aux fichiers de police et de sécurité enregistrent encore une très forte progression d'une année sur l'autre (+ 67 % en 1999 et + 21 % en 2000). Le nombre annuel de saisines se maintient en 2000 par rapport à l'année passée ; cette stabilisation intervient après une augmentation du nombre des saisines entre 1995 et 2000 de plus de 64 %.

LES DEMANDES DE CONSEIL

Depuis 1978, la CNIL a reçu plus de 10 000 demandes de conseil, dont 1 049 pour l'année 2000. Les secteurs d'activité qui ont suscité en 2000 le nombre le plus important de demandes de conseil concernent, par ordre décroissant, le travail, la santé, les collectivités locales, le commerce et tout particulièrement le commerce électronique, enfin, la fiscalité.

LES PLAINTES

Depuis 20 ans, la CNIL a reçu plus de 33 000 plaintes, dont 3 399 pour 2000. Les secteurs d'activité qui ont suscité le nombre le plus important de plaintes sont, par ordre décroissant, la prospection commerciale, le travail, la banque, les télécommunications, la santé, le crédit.

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.

LES AVERTISSEMENTS ET DENONCIATIONS AU PARQUET

L'instruction des plaintes conduit parfois 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 2000, la CNIL n'a délivré aucun avertissement (47 avertissements depuis 1978), mais a transmis une affaire à la justice, ce qui porte à 17 le nombre de dénonciations au parquet effectuées depuis 1978 (cf infra chapitre 2).

B. Le droit d'accès indirect

En application des articles 39 et 45 de la loi du 6 janvier 1978, toute personne a le droit de demander que des vérifications soient entreprises par la CNIL sur les renseignements la concernant pouvant figurer dans des traitements automatisés et des fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique. Aucun fichier de cette nature n'échappe à de telles vérifications. Les investigations sont effectuées par les membres de la Commission appartenant ou ayant appartenu au Conseil d'Etat, 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 5423 demandes de droit d'accès indirect qui ont donné lieu à 8978 investigations.

	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	**2000**
Requêtes	182	562	531	374	282	243	320	385	401	671	**817**
Evolution (en %)	+1,64	+2,09	-5	-29	-25	- 14	+ 31	+ 20	+ 4	+ 67	**+ 22**

La CNIL est saisie de demandes de droit d'accès aux fichiers de « police » ou de « renseignements » en nombre croissant (+ 22 % de 1999 à 2000), après une progression inédite (+ 67 %) entre 1998 et 1999. Les fichiers de police judiciaire, notamment le fichier STIC (cf infra chapitre 3), le fonctionnement en « vitesse de croisière » du système Schengen, de même que l'accès aménagé aux fichiers des renseignements généraux expliquent cette forte augmentation.

Les 817 demandes reçues par la CNIL en 2000 ont conduit la Commission à accomplir 1313 vérifications ; ces vérifications ayant été effectuées à hauteur de 90 % dans des fichiers relevant du ministère de l'Intérieur.

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 dans la crainte que des faits anciens n'entrave leur embauche,
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 judiciaire.

Ces vérifications ont concerné :

Ministère de l'Intérieur	**1 191**
- renseignements généraux (RG)	365
- police judiciaire (PJ)	123
- police urbaine (PU)	120
- direction de la surveillance du territoire (DST)	65
- direction de la sûreté et de la protection du secret (DSPS)	14
- système d'information Schengen (SIS)	504
Ministère de la Défense	**122**
- gendarmerie nationale (GEND)	*55*
- direction de la protection de la sécurité de la défense (DPSD)	33
- direction générale de la sécurité extérieure (DGSE)	34
Total	**1 313**

Le résultat des investigations menées en 2000, qui à l'exclusion de celles relatives aux renseignements généraux (365) et du système d'information Schengen (504) sont au nombre de 444, est le suivant :

Service	PJ	PU	DST	DSPS	GEND	DPSD	DGSE	**Total**	% du total
pas de fiche	31	89	*57*	8	38	21	31	**275**	62,00
fiche sans suppression d'informations	72	28	8	5	16	12	3	**144**	32,40
suppression totale ou partielle d'informations	16	3	_	1	1	_	_	**21**	4,72
mise à jour de la fiche	4	-						**4**	0,90
Total	123	120	65	14	55	33	34	**444**	100,00

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'Etat, la défense et la sécurité publique et qu'elles peuvent dès lors être communiquées au demandeur.

En pratique, trois situations peuvent se présenter :

1 — Les renseignements généraux ne détiennent aucune information nominative concernant un requérant ; dans ce cas, la CNIL en informe ce dernier, en accord avec le ministre de l'Intérieur.

2 — Les renseignements généraux détiennent des informations nominatives concernant un requérant ; les informations qui ne mettent pas en cause la sûreté de l'Etat, la défense et la sécurité publique lui sont communiquées, en accord avec le ministre de l'Intérieur. Dans l'hypothèse d'une communication totale ou partielle d'un dossier, le requérant a la possibilité de rédiger une note d'observation que la 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'Etat, 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 périmées. Le président de la CNIL adresse ensuite au requérant une lettre recommandée lui indiquant que conformément aux termes auxquels la CNIL est tenue en application de l'article 39 de la loi, « il a été procédé aux vérifications ». Cette lettre mentionne que la procédure administrative est close et indique les voies et délais de recours contentieux qui sont ouverts au requérant.

Bilan des 365 investigations menées en 2000 dans les fichiers des renseignements généraux :

	Investigations RG 2000	% du total des vérifications effectuées aux RG
Requérants non fichés aux RG	261	71 %
Requérants fichés aux RG	104	29%
Total	**365**	**100%**

Sur les 104 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	18	17%
Communication refusée par le ministre de l'Intérieur	0	
Communication acceptée par le ministre de l'Intérieur — communication totale — communication partielle	86 85 1	83 %
Total	**104**	**100%**

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 communication des pièces communicables du dossier s'effectue au siège de la CNIL lorsque le requérant est domicilié dans la région Ile-de-France ou, lorsque, domicilié dans une autre région, il fait 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 86 communications intervenues en 2000, 34 ont eu lieu au siège de la CNIL et 52 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé. A la suite de celles-ci, 6 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 10 dossiers,
- la suppression partielle de 3 dossiers,
- la mise à jour de 2 dossiers.

ÉVOLUTION DES INVESTIGATIONS AUX RENSEIGNEMENTS GÉNÉRAUX

Année	1992	1993	1994	1995	1996	1997	1998	1999	**2000**
Nombre de demandes traitées	766	320	273	197	252	352	282	270	**365**
Requérants non fichés aux RG	421	177	164	113	145	213	169	173	**261**
(% du total des vérifications)	*55 %*	*55 %*	60 %	*57 %*	58 %	60 %	60 %	64 %	**71** %
Requérants fichés aux RG	345	143	109	84	107	139	113	97	**104**
(% du total des vérifications)	45 %	45 %	40 %	43 %	42 %	40 %	40 %	36 %	**29 %**
Dossiers jugés non communicables	90	50	44	25	33	*57*	23	15	**18**
(% sur le nombre de requérants fichés)	26 %	35 %	40 %	30 %	31 %	41 %	20 %	15,5 %	17 %
Communication refusée par le ministre de l'Intérieur	13	0	0	0	0	0	0	0	**0**
(% sur le nombre de requérants fichés)	4 %								
Communication acceptée par le ministre de l'Intérieur	242	93	65	59	74	82	90	82	**86**
(% sur le nombre de requérant fichés) dont :	*70 %*	*65 %*	60 %	70 %	69 %	59 %	80 %	84,5 %	**83 %**
- communication totale	200	*75*	27	44	63	*75*	84	79	**85 (98,85**
- communication partielle	42	18	38	15	11	*7*	6	3	**1 (1,15 %)**

LES INVESTIGATIONS
CONCERNANT 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 des articles 109 et 114 de la convention Schengen, la CNIL a reçu **897 demandes d'accès aux fichiers du système d'information Schengen,** dont 397 pour la seule année 2000.

Année	1995	1996	1997	1998	1999	2000	**Total**
Nombre	22	20	21	78	359	397	**897**

Parmi les 897 demandes d'accès au N-SIS, 514 requérants étaient signalés.

Ces 514 signalements proviennent par ordre décroissant des pays suivants :

Pays signalant	Nombre de signalements	
Allemagne	246	47,8 %
France	199	38,7 %
Italie	40	7,8 %
Espagne	14	2,7 %
Pays-Bas	6	1,2 %
Grèce	4	0,8 %
Autriche	4	0,8 %
Belgique	1	0,2 %
	514	100,0 %

Suite aux démarches entreprises par la CNIL, **183 signalements ont été supprimés du N-SIS (35,6** %), dont 152 par l'Allemagne, 20 par la France, 6 par l'Italie, 2 par les Pays-Bas, 2 par l'Espagne et 1 par la Belgique.

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

BILAN 1978-2000

Au 31 décembre 2000, le nombre de traitements enregistrés par la CNIL depuis 1978 était de **753 676.** Les traitements déclarés selon une procédure simplifiée en représentent une part essentielle.

	1978-2000	% du total des formalités
Déclarations simplifiées	536 827	68,27 %
Demandes d'avis	41 362	5,26 %
Déclarations ordinaires	174 390	22,18 %
Demandes d'autorisation (chap Vbis - depuis 1997)	1 016	0,13 %
Demandes d'autorisation (chap Vter - depuis 1999)	81	0,01 %
Total des traitements enregistrés	**753 676**	-
Déclarations de modification	32 645	4,15 %
Total des formalités préalables	**786 321**	100,00 %

	1995	1996	1997	1998	1999	**2000**
Déclarations simplifiées	46 549	60 355	53 953	50 735	43 571	**33 657**
Demandes d'avis	2 765	3 269	2 724	3 002	3 538	**3 577**
Déclarations ordinaires	7812	9 727	10 326	11 333	12 200	**15 249**
Demandes d'autorisation (chap Vbis - depuis 1997)	-	-	133	244	352	**287**
Demandes d'autorisation (chap Vter - depuis 1999)	-	-	-	-	8	**73**
Déclarations de modification	1 777	3 428	2 639	2 358	3 454	**2 607**
Totaux	**58 903**	**76 779**	**69 775**	**67 672**	**63 123**	**55 450**

2000

Pour la période du 1er janvier au 31 décembre 2000, la CNIL a enregistré **55 450 nouveaux dossiers de formalités préalables,** dont 2 607 concernent des déclarations de modification de traitements déjà enregistrés. A l'instar des années passées, la progression des déclarations ordinaires émanant du secteur privé (+ 25 %) et des demandes d'avis du secteur public (+ 1,10 %) se poursuit.

	2000	% du total	rappel 1999	variation
Déclarations simplifiées	**33 657**	60,70 %	43 571	- 22,75 %
Demandes d'avis	**3 577**	6,50 %	3 538	+ 1,10 %
Déclarations ordinaires	**15 249**	27,52 %	12 200	+ 24,99 %
Demandes d'autorisation (chap Vbis - depuis 1997)	**287**	0,53 %	352	- 18,46 %
Demandes d'autorisation (chap Vter - depuis 1999)	**73**	0,03 %	8	+ 812,50 %
Déclarations de modification	**2 607**	4,72 %	3 454	- 24,52 %
Totaux	**55 450**	100,00 %	67 672	- 18,06 %

Demandes d'avis

Au cours de l'année 2000, la CNIL a délivré deux avis défavorables relatifs à des contrôles d'accès réalisés par le biais des empreintes digitales (cf infra chapitre 4) et plusieurs avis assortis de réserves.

Demandes d'autorisation

En 2000, la CNIL a délivré 73 autorisations en application du chapitre V ter de la loi du 6 janvier 1978.

Déclarations des sites Internet

Dans un souci constant de sensibiliser les responsables de sites aux questions de protection des données personnelles, la CNIL a multiplié les initiatives.

Ainsi, après avoir dévoilé à l'ouverture de son site web (www.cnil.fr) comment chacun est pisté sur la toile — « Vos traces sur Internet », module à présent décliné dans une version destinée aux juniors—, 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 100 sites de commerce électronique (2000) et de 60 sites de santé (2001), avant d'ouvrir à une large consultation publique un rapport sur la cybersurveillance des salariés (2001).

La CNIL a enregistré en 2000, 4 943 déclarations de sites Internet. Ce sont ainsi 8 702 sites Internet qui ont été recensés à la CNIL au 31 décembre 2000.

	1997	1998	1999	**2000**	**Total**
Déclarations sites Internet	267	930	2 562	**4 943**	**8 702**

D. Les visites, 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.

A 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 de fichiers des données personnelles.

En 2000, la CNIL a ainsi procédé à une trentaine de contrôles sur place et a effectué de nombreuses missions de vérification. La CNIL a notamment effectué plusieurs visites sur place avant de rendre son rapport sur le développement des sites web santé (cf infra chapitre 6) ou sur la lutte contre la fraude en matière de crédit (cf infra chapitre 7). Le secteur du logement social, qui fait l'objet de nombreuses saisines ou plaintes auprès de la Commission, a également conduit la CNIL à procéder à plusieurs missions de contrôle auprès d'organismes bailleurs (cf infra chapitre 2).

II. LES CHANTIERS LEGISLATIFS EN ATTENTE

L'entrée dans la société de l'information n'est pas seulement un slogan. Le nombre de personnes connectées, l'augmentation considérable du nombre de sites web, tout particulièrement de commerce électronique, le développement de la santé (cf chapitre 6) et la mise en place par les services publics et les collectivités locales de

procédures de télédéclarations destinées à faciliter les démarches administratives de nos concitoyens en témoignent.

A. La protection des données personnelles au cœur de la société de l'information

La protection des données personnelles et la sécurisation des transactions sont évidemment une préoccupation centrale des acteurs de la société de l'information. A cet égard, les mesures de libéralisation du chiffrement et la loi 2000-230 du 13 mars 2000 relative à la signature électronique ont constitué des étapes décisives pour assurer la confiance. De son côté, le conseil ou l'expertise de la CNIL, tout particulièrement en matière de sécurité, qu'il s'agisse des modalités d'authentification, de l'exigence de non répudiation ou de la confidentialité des données échangées, a été sollicité à diverses reprises par les pouvoirs publics. Ainsi, le ministère de l'Intérieur a consulté la CNIL dans le cadre d'une étude à caractère prospectif relative à la télétransmission des actes administratifs pris par les collectivités locales et soumis au contrôle de légalité vers les préfectures ou les sous-préfectures. La Commission est également saisie d'une demande d'avis par la direction de la comptabilité publique qui développe, dans le cadre du projet ACCORD, une dématérialisation complète des pièces justificatives entre ordonnateurs et comptables, le contrôle financier devant tendre vers le « zéro papier ». Une vraie révolution des pratiques administratives que le protocole TCPIP autorise ! Enfin, la CNIL a été saisie par la direction générale des impôts de la mise en œuvre à titre expérimental d'un système de déclaration par voie électronique des revenus des particuliers, expérimentation qui a offert l'occasion à la Commission de formuler, dans l'attente des décrets d'application de la loi sur la signature électronique, plusieurs recommandations pour régler les délicats problèmes d'authentification et mieux assurer la sécurisation des transmissions. Parallèlement, la migration vers Internet des procédures de déclarations électroniques propres aux entreprises, notamment les déclarations de résultat et le transfert de données fiscales et comptables se poursuit, Internet permettant en outre désormais de déclarer la TVA. Les délibérations rendues durant l'année sur l'ensemble de ces sujets, annexées au présent rapport, illustrent les modes d'intervention et les recommandations de la CNIL en cette matière.

Mais Internet ne concerne pas seulement les procédures de télédéclarations. Dans le cadre de ses missions générales, la Commission veille avec une attention particulière au respect des droits des internautes et tout particulièrement de leur droit d'accès aux informations les concernant et leur droit de s'opposer à une exploitation commerciale, au profit des tiers, des données qu'ils auront communiquées à un site web. Après l'évaluation de 100 sites de commerce électronique, la Commission accueille très favorablement les initiatives professionnelles tendant à mieux faire assurer la protection des données personnelles sur Internet. Elle a, à ce titre, examiné plusieurs référentiels d'organismes de labellisation qui comportaient des dispositions particulières en matière de protection des données personnelles et fait adopter par le groupe des autorités européennes de protection des données personnelles, institué

par l'article 29 de la directive du 24 octobre 1995, des recommandations communes de protection des données personnelles par les sites web.

Enfin, au delà des recommandations et rapport de consultation publique qu'elle a rendus sur deux importants sujets, les sites de santé d'une part, la cybersurveillance des salariés d'autre part — thèmes évoqués dans la suite de ce rapport — la Commission a entrepris deux études d'ensemble, en liaison avec les professionnels concernés mais aussi avec les associations de consommateurs ou d'internautes, l'une sur les problèmes particuliers qu'est susceptible de poser la diffusion sur Internet des décisions judiciaires lorsqu'elles comportent le nom et l'adresse des personnes, l'autre sur la protection de l'enfance et Internet. Ces deux études devraient être prochainement rendues publiques.

Mais si le développement grand public d'Internet et ses usages notamment commerciaux ont considérablement élargi le champ d'intervention de la Commission, et très certainement orienté ses pratiques et ses méthodes de travail, il demeure que les interventions de la Commission sont sans doute fragilisées par le retard pris par la France dans la transposition de la directive du 24 octobre 1995, instrument indispensable à l'adaptation de l'autorité de contrôle à ses nouvelles missions et au développement des nouvelles technologies. Où en sont les chantiers législatifs en attente ?

B. La réforme attendue de la loi du 6 janvier 1978

Le Gouvernement a souhaité recueillir l'avis de la CNIL sur l'avant-projet de loi appelé à modifier la loi du 6 janvier 1978 et à transposer la directive européenne du 24 octobre 1995. La Commission a rendu son avis le 26 septembre 2000. A la date de rédaction du présent rapport d'activité, le projet de loi est en cours d'examen par le Conseil d'Etat.

Les principales modifications que le projet de loi devrait apporter au dispositif d'ensemble de la loi du 6 janvier 1978 sont dictées *par* les prescriptions de la directive européenne :

— allégement des formalités de déclaration et de contrôle a *priori* des traitements automatisés de données à caractère personnel,

— suppression de toute distinction entre traitements selon qu'il s'agit de traitements publics ou privés,

— accroissement des pouvoirs de contrôle a *posteriori* du fonctionnement des fichiers et des traitements mis en oeuvre,

— énumération limitative des traitements (publics ou privés) qui, en raison de leur finalité ou des risques particuliers que leur mise en oeuvre est susceptible de présenter, feront l'objet d'un examen préalable,

— renforcement des mesures d'information des personnes concernées sur la finalité des traitements et sur leurs droits, tout particulièrement leur droit de s'opposer à toute utilisation à des fins de prospection commerciale des informations collectées, soit par le responsable du traitement lui-même, soit par les tiers auxquels ces informations ne

pourront d'ailleurs être cédées ou transmises que si les personnes concernées ont été préalablement mises en mesure de s'y opposer,

— renforcement du dispositif de garanties prévues en matière de flux transfrontières de données hors d'Europe.

S'agissant des options ménagées par la directive européenne sur divers points à l'égard desquels chaque Etat-membre dispose d'une large marge d'appréciation, il doit être souligné que le projet de loi, tel qu'il a été transmis à la CNIL, prévoit, comme cela avait été publiquement annoncé lors de la phase préalable de consultation publique, que l'autorité de contrôle disposerait de pouvoirs nouveaux de sanctions administratives, et tout particulièrement, à l'égard du moins des personnes morales de droit privé tirant profit du commerce des données, du pouvoir d'infliger des sanctions pécuniaires. La Commission approuve cette orientation.

S'agissant enfin des traitements n'entrant pas, ou que très partiellement, dans le champ d'application de la directive européenne — essentiellement les traitements dits de « souveraineté » — il est, à ce stade, envisagé d'introduire des dérogations à l'exercice du droit d'accès à certains traitements mis en oeuvre dans le cadre d'une mission de prévention, de recherche et de constatation des infractions fiscales et douanières ou de recouvrement des impositions lorsque la communication des données en cause serait de nature à faire obstacle à l'accomplissement de ces missions. La Commission n'est pas, dans son principe, opposée à de telles dérogations dès lors que leur champ d'application serait cantonné et que les traitements en cause demeureraient soumis à l'avis préalable de l'autorité de contrôle.

S'agissant en revanche du droit d'accès aux traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique, à l'égard desquels l'exercice de ce droit ne permet pas à la personne concernée, à l'heure actuelle et sous la seule réserve du dispositif particulier prévu pour les fichiers des renseignements généraux, de savoir s'il elle est fichée ou non, ni si les investigations menées par la CNIL ont abouti à des rectifications ou à des suppressions d'informations, le projet de loi autoriserait, dans certaines conditions, que la personne concernée soit informée des rectifications intervenues. La Commission approuve ce souci de plus grande transparence et estime que, dans bien des cas, les personnes devraient pouvoir se voir communiquer les informations les concernant sans qu'il en résulte d'atteinte aux intérêts en cause. Aussi, a-t-elle fait au Gouvernement des propositions tendant à élargir le dispositif proposé et à renforcer davantage la transparence.

S'agissant des traitements qui devraient, selon elle, suivre le régime prévu d'autorisation et parmi lesquels le projet de loi mentionne notamment certains traitements comportant des données sensibles, des données génétiques, les traitements comportant des informations relatives aux infractions, condamnations et mesures de sûreté, les traitements dont la finalité a pour effet d'exclure certaines personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, les traitements portant sur la totalité ou la quasi totalité de la population ou comportant le NIR (s'il s'agit dans ce dernier cas de traitements autres que sociaux ou fiscaux), la Commission a fait connaître son souci que puissent être soumis à ce même régime d'autorisation les traitements qui comportent des informations identifiant la nature, réelle ou supposée, des difficultés sociales des personnes, les traitements qui incluent les données

biométriques, les traitements dont la finalité pourrait justifier qu'il soit dérogé au droit d'accès. Enfin, la Commission estime que tous les traitements qui incluent l'interconnexion ou toute autre forme des mises en relation des données avec d'autres données traitées pour des finalités différentes devraient être soumis à ce nouveau régime d'autorisation.

S'agissant des traitements publics qui demeureront soumis à examen préalable de la CNIL (principalement les traitements de police, de justice, ceux qui comporteront le NIR ou qui concerneront la quasi totalité de la population), la Commission a émis le souhait que dans les circonstances où la loi du 6 janvier 1978 exige aujourd'hui un avis conforme de la CNIL et du Conseil d'Etat ou un avis favorable de la CNIL, il soit prévu soit un avis publié (au lieu et place d'un avis conforme), soit que seul un décret en Conseil d'Etat pourrait passer outre à un avis défavorable de la CNIL.

Au-delà d'observations qui, se rapportant à un projet de loi, revêtent nécessairement un caractère apparemment technique, la Commission a souhaité ainsi préciser les trois évolutions qui lui paraissent rendre nécessaire — et il faut bien le reconnaître, désormais urgente — l'adaptation de la loi du 6 janvier 1978 à l'évolution des techniques.

La première évolution, déjà ancienne, est l'extension de l'informatique et des nouvelles technologies à la sphère marchande.

Il y a 20 ans, les fichiers informatiques étaient principalement ceux de l'Etat et des grandes administrations. Désormais, des gisements considérables de données personnelles sont constitués et utilisés par les entreprises, notamment à des fins de prospection commerciale, et ont acquis, de ce fait, une valeur marchande.

Cette évolution justifie qu'il soit mis fin au double régime qui caractérisait la loi de 1978 (examen préalable des traitements publics, simple déclaration des traitements privés) et que les procédures de formalités préalables à la mise en oeuvre des traitements — sans doute adaptées au paysage informatique des années 80 — soient dans de nombreux cas allégées et simplifiées.

Dans le même temps, les enjeux financiers désormais liés à l'exploitation des bases de données commandent de rechercher des modes d'intervention propres à assurer que le respect de la vie privée des personnes et de leurs libertés individuelles ne se trouve pas mis en péril par la convoitise que peuvent susciter la collecte et l'exploitation des données personnelles (comportement d'achats, profils, etc.) ou la concurrence à laquelle se livrent les entreprises sur ce terrain.

La deuxième évolution, sans doute plus récente mais irréversible, est la convergence technologique.

Internet qui véhicule, selon les mêmes protocoles, texte, image et son, en est l'illustration manifeste, comme d'ailleurs les architectures en réseau, le développement des cartes à puce, de la vidéosurveillance, les usages possibles des « webcams » et les nouveaux services de téléphonie fixe ou mobile qui reposent sur l'exploitation de données de connexion ou de commutation au réseau. Aussi, les valeurs à protéger ne le sont-elles plus uniquement à l'égard de l'informatique *stricto*

sensu, c'est-à-dire d'une technique prise isolément, ni des fichiers traditionnels. La seule substitution de la notion de « données à caractère personnel » retenue par la directive à celle d'« informations nominatives » ne suffit pas à donner sa mesure au phénomène. C'est pourquoi le projet devrait davantage s'attacher à manifester que la protection des données personnelles et de la vie privée doit être garantie, quelles que soient les techniques concernées.

La troisième évolution est l'internationalisation de la protection des données.

A l'heure d'Internet et des développements des échanges internationaux de fichiers informatiques, l'application des lois nationales pouvait s'avérer, sinon vaine, du moins insuffisante à assurer un haut niveau de protection lors des transferts de données à destination de pays tiers. Loin d'abandonner la protection des données aux seules forces du marché mondial, l'Union européenne s'est accordée sur un socle commun de garanties dont l'objectif est double : permettre la libre circulation des données personnelles au sein de la Communauté européenne et inciter les autres pays du monde à adopter des dispositifs de protection comparables, sous peine de voir interrompu le fonctionnement continu des échanges internationaux d'informations.

Cette action a jusqu'à présent été couronnée de succès : tous les Etats membres de l'Union européenne sont désormais dotés de lois « Informatique et Libertés » ; hors d'Europe, de nombreux pays ont suivi cet exemple ; très récemment encore, les négociations engagées entre l'Europe et les Etats-Unis sur les flux transfrontières de données ont dégagé un compromis favorable à l'approche européenne.

L'internationalisation des échanges, loin de devoir conduire à relativiser la portée des principes et garanties reconnus en France depuis plus de 20 ans ou à faire douter de leur pertinence, doit impérativement inciter à les voir confirmés et élargis par la loi nouvelle, comme d'ailleurs la directive européenne l'a fait en consacrant sur de nombreux points l'expérience française.

C'est pourquoi l'adaptation des procédures aux évolutions constatées depuis 20 ans, et tout particulièrement l'abandon d'un examen systématique et préalable de tous les traitements automatisés de données personnelles, ne doit pas avoir pour effet d'abaisser le niveau de garanties jusqu'à présent reconnu dans la mise en œuvre par l'Etat de certains fichiers ou traitements de données particulièrement sensibles (fichiers de police, interconnexions de fichiers publics) à l'égard desquels la loi du 6 janvier 1978 a prévu, dans le souci d'apaiser les craintes qu'ils pouvaient légitimement susciter, des mécanismes de contrôle rigoureux.

Il appartiendra, en tout état de cause, au législateur d'arrêter les termes et le dispositif d'ensemble de la future loi. La Commission ne peut qu'émettre le vœu, compte tenu de la rapidité de l'évolution des techniques, que la future loi soit bien une loi d'avenir, énonçant les principes généraux, désormais communs à l'ensemble de l'Union européenne, et reposant sur la confiance à l'égard de la future autorité de contrôle afin que la loi nouvelle puisse conserver une souplesse suffisante qui seule en assurera la permanence. C'est en ces termes, et dans cet esprit, que la

Commission a présenté ses observations au Gouvernement : « Mais l'autorité de contrôle doit également continuer, comme elle l'a fait depuis 20 ans, à éclairer, non seulement les pouvoirs publics, mais aussi les citoyens sur les incidences des nouvelles technologies sur les droits fondamentaux des personnes et, notamment, sur le droit au respect de la vie privée. Lieu de veille technologique et éthique, lieu ouvert de concertation et de débats, l'autorité de contrôle devrait pouvoir organiser des consultations publiques sur des thèmes d'intérêt général relevant de ses attributions et, de manière plus générale, intervenir dans le débat public pour susciter la réflexion, ou hâter les évolutions ». Organe de la « conscience sociale » selon le vœu du président Tricot, la CNIL devrait être perçue au moins autant, si ce n'est plus, comme « vigie » que « vigile ».

Puisse ce vœu être entendu.

C. L'avis de la CNIL sur le projet de loi sur la société de l'information

Le Gouvernement a saisi la CNIL le 30 mars 2001 du projet de loi sur la société de l'information. D'autres autorités ou organismes ont également été saisis. Ce projet de loi, fort attendu, devrait être débattu au Parlement au cours de la présente cession. La CNIL rend public l'avis qu'elle a émis comme une contribution au débat.

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

La Commission nationale de l'informatique et des libertés, Saisie pour avis par le garde des Sceaux et le secrétaire d'Etat à l'Industrie, le 30 mars 2001, du projet de loi sur la société de l'information. Vu la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 ;

Vu la convention 108 du 28 janvier 1981 du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Vu la directive européenne 95/46 du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive européenne n° 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ;

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

Après avoir entendu M. Michel Gentot, en son rapport et M. Michel Capcarrère, commissaire-adjoint du Gouvernement, en ses observations, **Émet l'avis suivant**

Le projet de loi sur la société de l'information aborde plusieurs sujets concernant Internet qui correspondent aux débats de fond que le développement

du réseau suscite depuis plusieurs années dans l'ensemble des pays développés.

La CNIL se réjouit que ces débats puissent être tranchés, grâce à cette initiative législative destinée à adapter les règles de notre droit à la société de l'information, par le Parlement.

Elle rappelle que l'un des premiers débats qu'Internet a provoqués tenait à l'interrogation sur la portée ou l'efficacité de l'application d'une législation nationale à un réseau international. Aussi, souhaite-t-elle souligner que, dans le domaine de compétence qui est le sien, deux directives européennes (la directive du 24 octobre 1995 sur la protection des données personnelles et la libre circulation de ces données et la directive du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications) ont établi un socle de principes communs à l'ensemble des Etats membres de l'Union européenne, applicables à Internet. Plusieurs pays tiers se sont d'ailleurs, depuis lors, largement inspirés de ces principes, soit en adoptant des dispositions législatives destinées à assurer la protection des données personnelles, soit en développant des mécanismes d'auto-régulation poursuivant la même fin, lorsque le recours à de tels moyens d'agir correspondait davantage à leur manière de faire.

Ainsi, la protection des données personnelles et de la vie privée, qui faisait encore figure d'exception au moment de l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, est devenue la règle commune en Europe. En outre, les préoccupations que l'usage grand public ou commercial du réseau ont par ailleurs suscitées, à peu près dans les mêmes termes partout dans le monde, ont fait d'Internet un puissant vecteur de transmission de la culture européenne de protection des données personnelles. Aussi la CNIL est-elle très attentive aux choix auxquels le projet de loi procède et qui auront, à n'en pas douter, un écho particulier compte tenu de l'influence française en ce domaine.

La Commission croit à cet égard devoir souligner que sous des abords qui peuvent paraître techniques, plusieurs dispositions de ce projet touchent à des sujets qui excèdent très largement les spécificités de la technologie et qui concernent l'ensemble de nos concitoyens.

Ainsi, en est-il tout particulièrement pour l'usage, policier ou commercial, qui peut être fait de données personnelles qui relèvent par nature de notre vie privée et qui sont traditionnellement protégées par le secret de nos correspondances, le secret des choix audiovisuels ou l'inviolabilité de notre domicile. Il en est de même pour la diffusion d'une information personnelle sur le réseau international qui concerne non seulement les internautes mais toute personne dont le nom figure sur le Net.

En effet, les protocoles de communication utilisés par Internet produisent des « traces » sur notre comportement ou nos habitudes qui sont détenues par des tiers, intermédiaires techniques, tels que les opérateurs de communication, les fournisseurs d'accès et les hébergeurs de sites. Le volume des fichiers ainsi constitués et les possibilités d'exploitation des informations qu'ils comportent sont sans précédent. Aussi la question de l'utilisation qui peut être faite de telles données est-elle d'abord un débat sur la liberté dans une société numérique. Ce débat met naturellement en jeu, voire en conflit, non seulement les nécessités d'ordre public et le respect de la vie privée mais aus-

si la liberté du commerce et de l'industrie, ses exigences et les limites qu'imposent les capacités inédites de « ciblage », de « profilage » et de « pistage ».

La capacité de diffusion des informations sur le réseau est également sans précédent. On ne peut que se réjouir de l'élargissement considérable du périmètre de la liberté d'information et de l'accès aux savoirs qui en résulte. Cependant la technologie n'est pas neutre : il n'y a pas de commune mesure entre l'affichage d'un document à la porte d'un tribunal ou d'une mairie et sa diffusion sur Internet. Avec Internet, toute information diffusée en clair devient accessible depuis quelque endroit du monde que ce soit, sans que la profusion des informations disponibles ne constitue même une limite puisque les moteurs de recherche permettent de la retrouver dans l'instant. Cette possibilité technique de diffuser, dupliquer, récupérer, à l'échelle du monde, toute information disponible sur le réseau renouvelle sans doute les termes du débat sur la portée des mesures de publicité qui doivent entourer certaines informations lorsque ces dernière revêtent un caractère nominatif. C'est la raison pour laquelle, au-delà de l'avis que le Gouvernement a, en particulier, demandé à la Commission sur les dispositions du projet relatives à la publicité non sollicitée et à la conservation des données de connexion, la CNIL fera part de ses réflexions sur les dispositions du Titre Ier du projet relatives à l'accès à l'information.

Possibilités nouvelles d'exploitation des traces informatiques sur nos activités, possibilités sans précédent de diffusion de l'information à l'échelle mondiale : dans ces deux cas, la Commission estime que la recherche de l'intérêt général devrait s'inspirer d'une exigence de retenue. Les possibilités d'intrusion de la vie privée n'étant, désormais, nullement limitées par la technologie qui, bien au contraire, les facilite à un degré jusqu'alors jamais atteint, cette exigence pourrait clairement signifier que les autorités de l'Etat mais aussi les professionnels concernés ne s'autoriseront pas à faire tout ce que permet la technologie. Loin de toute « diabolisation » d'Internet, cette retenue devrait être perçue comme le prolongement naturel du principe de proportionnalité.

Dans cet esprit, la Commission se félicite que le principe de la liberté d'utilisation des moyens de cryptologie, y compris lorsque ces derniers recouvrent une fonction de confidentialité, soit consacré par la future loi, une telle mesure étant incontestablement décisive pour assurer la confiance.

En conséquence, les observations de la Commission porteront successivement sur les problèmes liés à la conservation des données de connexion, la publicité par la voie électronique, l'accès aux données publiques et l'accès aux archives publiques.

Conservation des données de connexion
(articles 17, 18 et 19 du projet de loi)

Le *dispositif prévu*

Le Titre II « De la liberté de communication en ligne » comporte un chapitre III, intitulé « L'effacement des données relatives aux communications », relatif à ce que l'on nomme communément, mais sous un vocable à coloration technique qui pourrait en dissimuler l'importance, les données de connexion, c'est-à-dire les informations qui sont produites ou nécessitées par

la technologie, qu'il s'agisse de nos communications téléphoniques ou de nos connexions au réseau Internet.

Les informations relatives à l'usage que l'on fait du téléphone ou d'Internet sont de celles qui touchent le plus intimement à notre vie privée : les personnes que l'on appelle, quand, d'où (avec le téléphone mobile), notre navigation sur Internet, les services que nous utilisons et les sites que nous consultons, l'heure exacte de nos communications ou de nos connexions, leur durée.

Cette matière est d'ailleurs si intimement liée à notre vie privée que les Etats membres de l'Union européenne ont estimé, au moment de l'ouverture à la concurrence du marché des télécommunications, qu'elle devait faire l'objet d'une réglementation spécifique et harmonisée. Tel est l'objet de la directive 97/66 du 15 décembre 1997 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications » que le projet de loi transpose dans notre ordre interne.

Le projet, qui vise les données de connexion dont disposent les opérateurs de téléphonie mais aussi les fournisseurs d'accès à Internet[1], pose le principe d'un effacement ou d'une anonymisation de « toute donnée technique relative à une communication lorsque celle-ci est achevée », transposant ainsi l'article 6 de la directive 97/66. Deux exceptions sont cependant ménagées pour prévoir, d'une part, que certaines données nécessaires à la Facturation ou au paiement de prestations pourront être conservés jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée, d'autre part et surtout, que certaines données pourront être conservées pendant une durée maximale d'un an, « pour les besoins de la recherche et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire de ces données ».

Le projet précise que les données qui seront conservées à de telles fins ainsi que, dans la limite prévue par la loi, leur durée de conservation seront précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, qu'en aucun cas ces données ne pourront porter sur le contenu des correspondances échangées ou des informations consultées, enfin que la conservation et le traitement de ces données devront s'effectuer dans le respect des dispositions de la loi du 6 janvier 1978. Le dispositif tel qu'il est arrêté par le projet de loi appelle plusieurs observations.

Observation générale

En évoquant, dans un même article, les données dont la conservation est justifiée par les nécessités de la facturation — ces données étant alors accessibles à la police judiciaire selon le droit commun — et celles dont la conservation, sans utilité pour l'internaute ou l'opérateur de télécommunication, sera prescrite par la loi à des fins exclusivement policières — c'est-à-dire, pris ensemble, le droit commun et l'exception — la présentation retenue par le projet de loi a pour effet d'estomper le caractère inédit du dis-

[1] Sont donc visées par ce texte les personnes physiques ou morales exploitant un réseau de télécommunications ouvert au public ou fournissant au public un service de télécommunication c'est-à-dire fournissant toute prestation incluant la transmission ou l'acheminement des signaux ou une combinaison de ces fonctions par des procédés de télécommunication.

positif retenu. Cet effet ne peut qu'être renforcé par l'apparent parallélisme qui est établi entre les modalités de conservation des données dans les deux hypothèses, pourtant bien distinctes : référence, dans les deux cas, à une durée de conservation d'un an[2], renvoi, dans les deux cas, à un décret en Conseil d'Etat pris après avis de la CNIL, référence commune aux dispositions de la loi du 6 janvier 1978.

Une telle présentation ne doit pas dissimuler les termes du débat important et légitime qui va être tranché par le législateur et qui concerne l'éventuelle utilisation par les services de police judiciaire des données liées à nos communications. L'enjeu est incontestablement d'importance à un moment où les pouvoirs publics souhaitent établir un cadre juridique suscitant la confiance pour l'entrée de la France dans la société de l'information. Si, selon une certaine approche, les potentialités d'Internet (rapidité des communications et volatilité des informations) nécessitent la mise en place de mesures particulières propres à éviter le développement par le réseau de certaines formes de délinquance ou d'atteintes aux droits des tiers, une autre approche consiste à soutenir qu'une technologie de communication et d'information ne doit pas déroger aux principes fondamentaux de l'Etat de droit qui méritent sans doute d'être adaptés aux spécificités d'Internet mais qui ne sauraient être considérés comme caducs par le seul effet de la nouveauté technologique.

Les termes de ce débat ne sont pas nouveaux, ni inédits en matière de nouvelles technologies. Ce fut d'ailleurs une des intuitions des législations de protection des données personnelles et de la vie privée, au premier rang desquelles figure la loi française du 6 janvier 1978 et la Convention du 18 janvier 1981 du Conseil de l'Europe pour la protection des données personnelles, que d'avoir prévu que l'informatisation de nos sociétés allait permettre la collecte, le stockage, la conservation et le traitement de données de plus en plus nombreuses sur nos comportements les plus intimes (l'usage d'une carte bancaire, la nature et le montant de nos achats, le lieu où l'on se trouve à tel moment, l'heure d'une connexion, le lieu d'où l'on passe un appel depuis un mobile, le passage à tel péage d'autoroute, etc.). Les nouvelles technologies contribuent à créer de nouveaux gisements de données qui constituent, pour la police, autant d'éléments de preuves aisément accessibles, lui offrant ainsi des possibilités d'investigation sans précédent. Aussi, ayant pressenti que les capacités de stockage et de traitement de l'information pourraient se développer quasiment sans connaître de limites techniques — ce qui est précisément advenu — le législateur a-t-il souhaité définir, dès les premiers balbutiements de la société numérique, des garanties destinées à prévenir toute rupture de l'équilibre entre les droits du citoyen et les prérogatives de l'Etat.

En subordonnant le traitement d'informations *nominatives au* principe de finalité (quelles données collectées et traitées et à quelles fins ?), en limitant la durée de conservation de ces données à ce que justifie la finalité des traitements en cause, en exigeant que les données conservées soient « pertinentes » et non « excessives » au regard de la finalité de la collecte et en imposant des mesures générales d'information des citoyens sur ces différents points, les lois de protection des données personnelles et de la vie privée ont

[2] Article L 32-3-3 nouveau du code des postes et télécommunications, § II pour les données conservées à des fins de police, article L 32-3-3 nouveau, § III et article L 32-3-5 nouveau pour les données de facturation.

décliné, à l'aube de la société de l'information, les principes fondamentaux de proportionnalité et de retenue qui avaient précédemment et successivement conduit l'Etat à s'interdire d'opérer des perquisitions de nuit au domicile d'un particulier, de saisir des objets ou des effets lui appartenant en enquête préliminaire sans son consentement exprès ou encore de le placer sous écoute téléphonique hors un cadre juridique rigoureux et dans certaines circonstances d'une gravité particulière dont l'appréciation est soumise au contrôle d'une autorité indépendante (l'autorité judiciaire pour les écoutes judiciaires, une autorité administrative indépendante pour les interceptions de sécurité).

Ces principes de protection des données personnelles n'ont nullement eu pour effet de priver la police de moyens d'action dans la mesure où, tout au contraire, ces derniers se sont développés, quasi mécaniquement, au fur et à mesure de l'informatisation de nos sociétés. C'est précisément la raison pour laquelle les législations de protection des données personnelles et de la vie privée ont posé le principe suivant : tant que des données personnelles sont conservées dans un traitement ou un fichier, elles demeurent accessibles à l'autorité judiciaire et à la police judiciaire. En revanche, sauf exception proportionnée et justifiée, des données à caractère personnel ne peuvent être conservées au-delà de ce que justifie la finalité de leur collecte ou de leur traitement initial.

Le projet de loi dérogeant à ces principes, le dispositif retenu mériterait d'être apprécié dans la plus grande clarté compte tenu des intérêts en cause.

Observations sur la conservation des données nécessaires à la facturation

S'agissant des opérateurs de téléphonie (fixe ou mobile), les données générées par nos communications (qui on appelle ? quand ? pendant combien de temps ? où ? d'où ?) sont fondamentalement liées à la facturation qui est d'ailleurs très largement déterminée par elles. Ces données sont évidemment particulièrement sensibles, mais nul ne met en cause la légitimité de leur conservation aussi longtemps que la facture peut être contestée. Sans doute la téléphonie mobile a-t-elle apporté une information supplémentaire par rapport aux informations « plus classiques » liées à la téléphonie fixe : notre localisation lorsque nous passons ou recevons un appel depuis un portable. S'agissant de ceux des fournisseurs d'accès à Internet dont la tarification du service est liée à un forfait, les données dont la conservation est justifiée par une nécessité de facturation sont plus limitées dans la mesure où le tarif des connexions à Internet est toujours celui d'une communication locale, quels que soient la distance du serveur auquel l'abonné se connecte, la nature du site web consulté ou l'identité du destinataire d'un message électronique. La CNIL a déjà appelé de ses voeux [3] une harmonisation de la durée de conservation de telles données. En effet, jusqu'à présent seul l'opérateur historique était tenu, en conséquence des dispositions de l'article L 126 du code des P et T, de ne les conserver que pendant une durée d'un an, les règles de droit commun en matière de prescription des créances civiles autorisant les opérateurs entrants à conserver ces informations pendant le délai ordinaire de prescription, soit 5 ans, durée qui pouvait, à tous égards et compte tenu

en particulier de la sensibilité des informations en cause, paraître tout à la fois excessive et susceptible de provoquer des atteintes injustifiées à la vie privée des personnes.

Aussi, la CNIL ne peut-elle qu'être favorable à ce que le projet de loi consacre le principe de finalité, principe cardinal de la protection des données personnelles et de la vie privée, en prévoyant que les opérateurs ne pourront conserver les données en cause pour les besoins de la facturation et du paiement des prestations que jusqu'à l'expiration de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et en fixant, pour tous les opérateurs, ce délai à un an. Il résultera d'un tel dispositif d'harmonisation un raccourcissement des durées de conservation actuellement pratiquées par certains opérateurs.

S'agissant d'une éventuelle utilisation de ces données par les opérateurs souhaitant commercialiser leurs propres produits et services, la Commission prend également note avec satisfaction qu'un traitement de ces données à de telles fins ne pourra être entrepris qu'avec le consentement exprès des personnes. Cette disposition, que commande la transposition de l'article 6 de la directive 97/66 du 15 décembre 1997, renforcera les garanties jusqu'alors offertes aux usagers, le droit actuel ne distinguant pas entre ces données et des données plus « classiques » telles qu'un nom ou une adresse. En revanche, le texte proposé laisse entier le problème de savoir si un tel consentement, une fois acquis, autoriserait ou non l'opérateur à conserver les données de facturation au-delà de la durée d'un an. Ce point mériterait incontestablement d'être éclairci.

De même, la CNIL prend note avec satisfaction qu'en aucun cas de telles données ne pourront être utilisées pour le compte de tiers et qu'enfin la conservation et le traitement de ces données seront soumis aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La Commission s'interroge toutefois sur la rédaction proposée pour l'article L 32-3-3 nouveau § III du code des postes et télécommunications (article 17 du projet) qui évoque l'hypothèse d'une transmission de ces données de facturation à des tiers. Outre l'apparente contradiction entre une telle hypothèse et les garanties ci-dessus rappelées, une telle précision pourrait paraître sans réelle portée dans la mesure où la référence faite à la loi du 6 janvier 1978 suffit à autoriser une telle transmission dès lors qu'elle serait justifiée par la finalité de facturation ou de recouvrement.

En définitive, le principe d'une conservation des seules données nécessaires à la facturation, la fixation de la durée de conservation de ces données à un an, quel que soit l'opérateur, ainsi que le renvoi à un décret en Conseil d'Etat pris après avis de la CNIL pour déterminer celles des données qui pourront être conservées à ce titre reçoivent l'approbation de la Commission.

Observations sur la conservation des données de connexion sans lien avec la facturation

. L'enjeu

Il convient d'emblée de relever qu'en faisant obligation aux opérateurs de télécommunications de conserver des données de connexion dépourvues d'uti-

lité pour la facturation, le projet de loi ne poursuit pas un objectif d'ordre public qui serait justifié par la nécessité d'identifier les auteurs de contenus illégaux ou attentatoires aux droits des tiers (sites pédophiles, négationistes, racistes, diffamatoires et autres). En effet, la loi du 1er août 2000 a déjà établi à la charge des hébergeurs de sites mais aussi des fournisseurs d'accès — visés ensemble par l'article 43-9 nouveau de la loi du 30 septembre 1986 — une obligation générale de « détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu », dans des conditions et pour une durée qui doivent être précisées par un décret en Conseil d'Etat pris après avis de la CNIL, les données ainsi conservées pouvant être requises par l'autorité judiciaire. Le projet de loi sur la société de l'information est de portée beaucoup plus large puisqu'il concerne tous les internautes qui échangent des mails ou naviguent sur le web, même s'ils ne créent aucun contenu accessible au public. Certes, le projet précise que les données ainsi conservées « ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit ». Mais cette rédaction, qui se borne à un constat exclusivement technique, si elle n'est pas inexacte, pourrait cependant donner à penser que de telles données sont anodines. Or, elles ne le sont nullement dans la mesure où, comme le précise le projet par ailleurs, elles portent notamment « sur l'identification des personnes utilisatrices des services fournis par l'opérateur de télécommunication ». Concrètement, il s'agit de faire obligation aux fournisseurs d'accès de conserver ce que l'on nomme les « adresses IP » des ordinateurs connectés aux services accessibles par Internet, adresses qui constituent l'équivalent d'un numéro minéralogique que le fournisseur d'accès attribue à l'ordinateur utilisé par l'abonné, soit de manière permanente, soit à chacune de ses connexions. La conservation de cette adresse IP permet d'identifier tout ordinateur connecté au réseau (et donc la personne physique titulaire de la ligne) et ses heures de connexion. Certes, à elle seule, la conservation de ces informations ne permet pas d'identifier l'activité de l'internaute. Mais si le projet de loi prescrit la conservation de telles données, c'est précisément pour associer à un comportement sur Internet une identité précise. La technologie d'Internet (c'est-à-dire le protocole de communication entre ordinateurs distants) permet déjà à certains robots de récupérer l'ensemble des adresses IP des ordinateurs connectés la conservation des données de connexion par les fournisseurs d'accès permettra d'identifier individuellement leurs utilisateurs ou tout au moins la personne physique titulaire de la ligne. De même, le rapprochement des données devant être conservées par les fournisseurs d'accès avec celles dont la loi du 1er août 2000 a prescrit la conservation aux hébergeurs de sites, permettrait d'identifier, non pas seulement les personnes ayant rendu un contenu accessible sur Internet, mais beaucoup plus généralement les internautes s'étant bornés à consulter tel ou tel site. Ces quelques précisions techniques donnent la mesure de ce qui est en cause dans le projet de loi : l'absolue et inédite transparence de notre activité d'internaute lorsque pourtant nous nous abstenons de mettre un contenu à la disposition du public via le réseau.

. Les termes du débat

Nul ne paraît contester la nécessité de prévoir des mesures de précaution afin de lutter contre certaines formes de délinquance ou de criminalité sur le

réseau, tout particulièrement en matière d'intrusion ou de propagation de virus informatique. Ce souci d'intérêt public nécessite, à n'en pas douter, la conservation par les fournisseurs d'accès des données de connexion. Mais c'est la portée des mesures à prévoir à cette fin et les garanties qui doivent les entourer qui font légitimement débat depuis plusieurs années entre les acteurs de la société de l'information et les pouvoirs publics dans l'ensemble des pays développés.

Compte tenu du caractère dérogatoire aux principes généraux de protection des données personnelles et de la vie privée et, de manière plus générale, des atteintes possibles au respect de la vie privée et des libertés individuelles qu'emporte la conservation à des fins exclusivement policières de données dépourvues d'utilité technique, une fois la connexion établie entre un internaute et son interlocuteur (qu'il s'agisse de la personne physique avec laquelle l'internaute communique par courrier électronique ou d'un serveur distant, support d'un site public d'information), la sagesse et le principe de proportionnalité que commande tout particulièrement l'article 6 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales devraient présider au débat public que le projet de loi ne manquera pas de susciter. Les intérêts en cause sont nombreux et de nature diverse.

S'agissant des impératifs de sécurité publique, ne sont pas en cause la prévention et la recherche des contenus illégaux accessibles au public (le dispositif légal institué par la loi du 1er août 2000 y répond déjà), mais celles des actes de délinquance que la communication par le réseau pourrait faciliter ou permettre.

Il est déjà possible aux autorités de l'Etat, dans les conditions prévues par la loi du 1er août 1991 relative au secret des correspondances émises par la voie des télécommunications, de procéder à des interceptions de communications sur Internet, comme elles peuvent le faire pour les communications téléphoniques, ce qui résulte d'ailleurs clairement de l'article 52 du projet de loi. De telles interceptions, placées sous le contrôle du juge ou d'une autorité indépendante, permettent déjà d'identifier les comportements délictuels ou criminels.

Le projet de loi n'a donc pas pour objet de rechercher un moyen de substitution à une technique qui ne serait pas applicable à Internet — l'interception est possible sur Internet — mais à étendre les possibilités dont devraient disposer les autorités publiques, en ajoutant aux moyens traditionnels dont elles disposent déjà (les interceptions de communication), des moyens nouveaux que la technologie et les protocoles de communication permettent de mettre en œuvre (le rapprochement et l'analyse des données de connexion).

S'il a pu être regretté par les autorités policières, dans tous les pays du monde, que certains fournisseurs d'accès ne conservent que durant quelques jours les données de connexion de leurs usagers, une telle situation ne doit pas faire perdre de vue le fait que la plupart des fournisseurs d'accès, en tout cas les plus importants, conservent, à des fins de sécurité informatique interne, les données de connexion de leurs abonnés pendant une durée de l'ordre de trois mois, ces données étant alors accessibles aux forces de police, dans le cadre des enquêtes judiciaires qu'elles diligentent. Imposer une obligation de conservation des données de connexion pendant un an, au motif que, jusqu'à présent et dans le silence de la loi, certains fournisseurs

d'accès ne conservaient ces données que durant quelques jours pourrait paraître, sur le terrain des libertés individuelles et publiques, manquer de mesure.

Il convient de mettre en regard des impératifs d'intérêt public, qui méritent donc d'être nuancés, **la liberté personnelle :** celle de consulter un site Internet sans avoir le sentiment d'être sous surveillance, celle de pouvoir adresser un message électronique, comme on adresse un courrier postal ou un appel téléphonique, non pas avec un sentiment particulier de liberté, tant celle-ci nous paraît acquise, mais sans calcul ni préoccupation. Le développement du minitel en France a suscité, en termes de libertés personnelles, des débats de même nature que ceux qui sont aujourd'hui abordés, s'agissant d'Internet. Ne convenait-il pas de se prémunir contre certains des usages « inconvenants » de la télématique, de veiller au respect de l'ordre public et d'une certaine civilité par les kiosques ? Le choix a pourtant été fait de ne pas lier la facturation à la nature des services offerts et de renoncer à installer une « mémoire vive »[4] dans les terminaux de sorte que la nature des services consultés par les usagers ne soit ni conservée, ni traitée. Et nul n'avance qu'en procédant ainsi l'Etat se serait désarmé face à certaines formes de délinquance. Il s'agissait, à l'heure d'une technologie jusqu'alors inédite, de s'en tenir aux principes fondamentaux de protection de la vie privée des personnes qui président également à l'accès aux services de communication audiovisuelle : en cette matière, le secret de ses choix, dans une société de libertés, devrait demeurer la règle et les exceptions très rigoureusement pesées.

Le dernier intérêt en cause, qui ne se situe pas sur le terrain des libertés mais qui mérite sans doute d'être évoqué, est celui **des fournisseurs d'accès** eux-mêmes, acteurs sans lesquels les connexions à Internet ne seraient pas possibles. Sans doute les contraintes d'une catégorie de professionnels ne sauraient-elles dicter ce que commande l'intérêt général. Cependant, c'est sur eux que pèsera, techniquement et financièrement, l'obligation de conserver pendant de longues durées les données de connexion. Les estimations les plus sérieuses évaluent le nombre de pages web consultées par jour, en France, à 4 ou 5 milliards. S'agissant des messages électroniques, l'Association des fournisseurs d'accès précise que les abonnés des professionnels qu'elle fédère auraient envoyé, pour la seule journée du 3 janvier 2001, 3 600 000 messages. De tels volumes donnent incontestablement la mesure de l'obligation qui leur serait faite s'ils étaient tenus de conserver pendant une durée d'un an trace de l'ensemble des connexions et du coût que représenterait, alors, la recherche de celles des données qui pourraient, les cas échéant, être utiles à une enquête. Il serait à craindre que le coût final d'une telle obligation soit reporté sur les internautes.

. L'appréciation de la Commission

L'obligation faite aux fournisseurs d'accès de conserver à des fins de police trace des connexions qui, par recoupement avec d'autres données, peuvent dévoiler notre navigation sur le web et, de manière plus générale, l'usage privé que l'on fait du réseau, déroge aux principes fondamentaux de protection des libertés individuelles. Dès lors, il convient que la loi édictant une

[4] Cf. 6e rapport d'activité de la CNIL pour 1985, p. 66 à 68.

telle obligation soit à la fois claire et précise et que le dispositif mis en œuvre soit adapté et proportionné.

Or, le projet de loi renvoie au pouvoir réglementaire le soin de déterminer les données en cause et leur durée de conservation précise, dans la limite maximale d'un an. Certes, la rédaction du projet de loi sur ce point laisse penser que la durée de conservation finalement retenue pourrait être, dans certains cas, inférieure à un an et que seules certaines données de connexion, et non pas toutes, seraient en définitive conservées.

Cependant, l'hypothèse d'un tri entre des données à caractère technique qui sont rassemblées dans des fichiers dits « fichiers log » peut paraître assez peu réaliste d'autant qu'un tel dispositif reviendrait à ajouter à la contrainte faite aux opérateurs de conserver des données sans utilité pour eux une deuxième contrainte consistant à leur demander de procéder à une sélection *a priori* entre les données produites par la technologie. D'autre part et surtout, l'obligation ainsi instituée dérogeant au droit commun, sa portée et ses modalités de mise en œuvre paraissent devoir être déterminées par le législateur. Il est en tout cas permis de s'interroger sur le point de savoir si un renvoi aussi général au pouvoir réglementaire, fut-ce après avis de la CNIL, offre les garanties de précision et de clarté exigées dans une matière qui touche aux libertés individuelles et publiques, étant observé qu'il ne s'agit plus, comme dans la loi du 1er août 2000, de permettre l'identification d'auteurs de contenus diffusés sur Internet mais toutes les personnes se connectant à Internet.

Sur le fond, la Commission estime que dans la mesure où la pratique des fournisseurs d'accès n'est pas aujourd'hui harmonisée et où certains d'entre eux ne conservent que très peu de temps les données de connexion, ce qui au demeurant ne peut que fragiliser la sécurité informatique de leurs propres installations, l'obligation nouvelle qui serait désormais faite à l'ensemble des fournisseurs d'accès de conserver les données de connexion pendant une durée de trois mois serait adaptée aux objectifs d'intérêt public poursuivis par le projet de loi.

La Commission croit devoir souligner que, selon le témoignage recueilli auprès de ses homologues européens, ceux des Etats membres ayant prévu une obligation de conservation de ces données pendant une durée maximale de cet ordre ne paraissaient pas avoir rencontré de problèmes particuliers en matière de lutte contre la délinquance par le réseau.

Par ailleurs, dans une résolution législative portant avis du Parlement européen sur le projet d'action commune relative à la lutte contre la pornographie enfantine sur Internet[5], cette Assemblée a estimé qu'une durée de conservation des données de trafic de trois mois pouvait être adaptée.

Enfin, la Commission européenne, saisie pour avis par la Belgique d'un projet de loi de réforme du code pénal qui retenait, notamment, une durée de conservation des données d'appels et d'identification des utilisateurs d'au moins douze mois, et qui renvoyait à des arrêtés royaux le soin d'arrêter les durées de conservation précises en fonction des services utilisés, a émis un avis circonstancié estimant que l'obligation ainsi définie était insuffisamment précise au regard des exigences européennes, qu'elle constituait une restric-

[5] JO C219 du 30 juillet 1999, p. 68 et p. 71.

tion excessive à l'exercice des activités économiques et une atteinte non justifiée aux principes de protection des données personnelles. L'ensemble de ces considérations conduit la CNIL à estimer qu'un délai de conservation de trois mois serait parfaitement proportionné et adapté aux intérêts en cause.

Enfin, les conditions dans lesquelles de telles données personnelles pourraient être saisies dans le cadre d'une procédure judiciaire mériteraient sans doute d'être précisées compte tenu de la nature particulière de telles données qui ne sont pas conservées par les personnes concernées par la communication, mais par un tiers (le fournisseur d'accès). En effet, le projet de loi, en son état, ne parait subordonner un tel accès à ces données à aucune condition tenant à la gravité de l'infraction recherchée et donne à penser que ces données pourraient être consultées ou saisies dans le cadre d'une enquête préliminaire qui se caractérise, pourtant, par le fait qu'à ce stade l'infraction n'est pas patente et ne permet pas à la police judiciaire de procéder à des saisies ou perquisitions, sans l'accord exprès des personnes concernées.

La publicité par voie électronique
(articles 25 et 26 du projet de loi)

Le *dispositif prévu*

Le Titre III « Du commerce électronique » comporte un chapitre II relatif à la publicité par voie électronique qui institue une obligation de transparence à l'égard des consommateurs par l'identification claire et non équivoque de la nature publicitaire des messages électroniques de publicité non sollicitée ainsi que des offres promotionnelles telles que les rabais, primes, cadeaux, concours ou jeux. Cette obligation est tout à fait satisfaisante.

Le projet de loi introduit par ailleurs dans le code de la consommation un article L 121 -15-3 nouveau faisant obligation aux personnes physiques ou morales utilisant la messagerie électronique des internautes pour leur adresser des messages publicitaires qu'ils n'ont pas sollicités de « veiller » à ce que de tels messages « ne soient pas adressés à des personnes physiques qui ne souhaitent pas recevoir ce type de communication et qui se sont inscrites à cet effet dans des registres d'opposition ». Le projet de loi renvoie à un décret en Conseil d'Etat le soin de fixer les conditions de fonctionnement de tels registres.

Les *enjeux*

Cette dernière disposition appelle plusieurs observations.

Elle tranche un débat auquel tous les internautes dans tous les pays sont extrêmement sensibles puisqu'il met en cause, à la fois, la nature d'Internet dont il paraît souhaitable qu'il ne soit pas considéré comme un outil à vocation exclusivement marchande, le sort des données personnelles et tout particulièrement l'utilisation à des fins commerciales des adresses électroniques que les internautes ont pu communiquer à de toutes autres fins dans les espaces publics de l'Internet (forum de discussion, liste de diffusion, etc.) et enfin la tranquillité de ceux qui peuvent souhaiter ne pas voir leur boîte aux lettres électronique inondée de messages indésirables, sans avoir à accomplir de démarche particulière à cet effet.

Ce débat qui s'est focalisé autour de ce que l'on nomme communément le « spamming » qui est la forme la plus controversée du publipostage électronique et qui consiste à adresser des messages électroniques à des centaines, des milliers, voire des millions de destinataires avec lesquels l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet, est beaucoup plus important qu'il n'y paraît. En effet, le publipostage électronique ne concerne pas le seul commerce électronique. Il peut être le support de communication de messages de nature très différente : prosélytisme religieux ou sectaire, messages à caractère pornographique, etc. Par ailleurs, les adresses électroniques des internautes ne sont pas toutes celles de personnes majeures : des mineurs peuvent être concernés.

Aussi convient-il que la règle de droit qui sera posée en la matière puisse prévenir toute dérive. En n'évoquant que la seule publicité commerciale, et en faisant obligation aux internautes ne souhaitant pas être sollicités de s'inscrire sur des registres d'opposition, le projet de loi dans sa rédaction actuelle pourrait laisser penser que serait régulier tout envoi de message non sollicité, quelle qu'en soit la nature, à l'égard d'une personne, quel qu'en soit l'âge, qui ne se serait pas inscrite dans un registre d'opposition. Une telle manière de voir, si elle devait prospérer, pourrait avoir des effets tout à fait désastreux, compte tenu notamment du nombre de jeunes adolescents disposant d'une adresse électronique.

Par ailleurs, la prospection électronique tire sa force des caractéristiques particulières d'Internet qui doivent être prises en compte au moment de légiférer sur le sujet. En effet, à la différence de la prospection traditionnelle, dans laquelle l'expéditeur supporte entièrement les frais de prospection (qu'elle soit postale, téléphonique ou par télécopie), la prospection électronique est quasiment à coût nul pour le prospecteur. Il est possible de se procurer sur Internet pour des sommes modiques des CD-Rom concernant jusqu'à 60 millions d'adresses électroniques. Les frais de production et de communication des messages sur Internet sont, grâce à la numérisation et aux possibilités de duplication immédiate qu'autorise la technologie, sans commune mesure avec les coûts élevés que nécessitent les envois postaux (fabrication de maquette, coût du papier, mise sous pli, affranchissement). Or, jusqu'à présent, le législateur, national ou européen, a toujours considéré que plus le coût de la prospection était faible pour le commerçant, plus les risques d'abus étaient réels, comme l'ont manifesté, tour à tour, la prospection téléphonique par automate d'appels (dans les années 80) et surtout la prospection par télécopie (dans les années 90).

C'est la raison pour laquelle l'Union européenne s'est accordée pour limiter l'usage de telles formes de prospection en subordonnant l'utilisation des automates d'appels et, désormais, de la télécopie à des fins de prospection au consentement de la personne concernée : sans consentement, ces modalités de prospection sont irrégulières.

Enfin, et surtout, le problème traité par le projet de loi ne se limite pas aux inconvénients qui s'attacheraient à la seule réception d'un message non sollicité par l'internaute. Il ne peut y avoir sur Internet d'envoi de messages que s'il y a eu précédemment collecte automatisée des adresses électroniques des internautes, c'est-à-dire, constitution de véritables bases de données dont l'ampleur a été soulignée ci-dessus. Telle est la pratique de certains opérateurs qui n'hésitent pas à lancer des robots sur Internet afin de récupérer toutes les

adresses électroniques disponibles sur les espaces publics d'Internet. Dès lors, l'adresse électronique utilisée, et éventuellement le « profil » de son titulaire tel qu'il peut être déduit des échanges que l'internaute considéré a pu librement avoir sur tel sujet particulier dans un forum de discussion, sont conservés, à son insu dans une base de données, à des fins commerciales ou de prosélytisme, par un tiers avec lequel il n'a jamais eu de contact. Soutenir que la mise en place de registres d'opposition constituerait une mesure suffisante revient à espérer qu'en évitant d'alarmer l'internaute, ce dernier n'exercera aucun des droits qui lui sont pourtant reconnus à l'égard des traitements de données personnelles le concernant : les données le concernant continueront à être traitées et, le cas échéant, cédées à des tiers mais, tenu dans l'ignorance du fait, il ne disposera plus d'aucun moyen de demander la radiation de ses coordonnées des fichiers dans lesquels elles figurent.

Au regard de ces trois caractéristiques, qui distinguent clairement la prospection électronique sur Internet d'autres formes plus classiques de prospection commerciale, on ne peut que s'interroger sur les justifications du dispositif prévu dans le projet de loi.

Sans doute la directive européenne 2000/31 dite «Commerce électronique », prévoit-elle la mise en place de tels registres d'opposition. Mais, contrairement à ce que soutiennent certains groupes professionnels, cette directive n'a aucunement entendu choisir entre les deux solutions qui ont été passionnément discutées sur le sujet, la première consistant à permettre que toute prospection électronique soit possible à l'égard des personnes qui n'auraient pas manifesté, par un geste positif, leur refus d'en recevoir (dite « opt out »), la deuxième soutenant au contraire que, compte tenu de ses caractéristiques, la prospection par courrier électronique était une des plus intrusives qui soient dans le monde du commerce et qu'il convenait, comme pour la publicité par automates d'appels ou par télécopie, d'en subordonner l'usage aux seules personnes qui y avaient consenti (dite « opt in »). En effet, l'article 7 de la directive concernée n'évoque que « les Etats membres qui autorisent les communications commerciales non sollicitées », signifiant ainsi clairement que le choix d'autoriser ou non de telles formes de publicité relevait du niveau national et n'était nullement imposé par la législation communautaire. La rédaction de cet article fait en outre une référence expresse aux « autres exigences prévues par le droit communautaire » parmi lesquelles figure la directive « protection des données personnelles » au 24 octobre 1995, le considérant 30 du texte européen précisant par ailleurs que « la question du consentement du destinataire pour certaines formes de communications commerciales non sollicitées n'est pas traitée par la présente directive ». Dès lors aucun argument tenant aux exigences communautaires n'impose à la France d'arrêter un tel dispositif.

L'appréciation de la Commission

La Commission ne peut, dans ces conditions, que rappeler les conclusions qu'elle a rendues publiques dans son rapport d'ensemble sur le sujet, adopté le 14 octobre 1999[6].

[6] Rapport « Le publipostage électronique et la protection des données personnelles » adopté par délibération du 14 octobre 1999 — www.cnil.fr

Outre les caractéristiques particulières de la prospection électronique qui ont été rappelées plus haut, la Commission souhaite souligner, qu'à la différence des autres formes de prospection, la prospection *par* courrier électronique est très « intrusive » et directement ciblée. Une boîte aux lettres électronique, à la différence d'une « boîte aux lettres physique », est directement ouverte sur le monde et dépourvue des « barrières » que constituent un hall d'entrée, un digicode ou une gardienne.

Par ailleurs, ce mode de prospection est coûteux pour les internautes, un récent document d'étude de la Commission européenne [7] évaluant à 10 milliards d'euros le coût annuel mondial supporté par eux au titre de la réception de messages non sollicités (le coût étant déterminé en fonction de la durée moyenne de lecture des messages avant effacement). C'est la raison pour laquelle la pratique du « spam » est vécue, par les internautes mais aussi par les fournisseurs d'accès à Internet dont les installations peuvent être utilisées à leur insu pour dupliquer un même message à des milliers d'exemplaires — encombrant ainsi, au détriment des usagers, le volume de la bande passante et donc la rapidité des connexions — comme une pratique intolérable.

Aussi, certains pays européens ont-ils subordonné l'usage de la prospection non sollicitée par courrier électronique, comme c'est déjà le cas pour la prospection par automates lanceurs d'appels ou par télécopie, au consentement des personnes. Telle est déjà la norme dans les deux pays européens qui connaissent le plus fort taux de pénétration de l'Internet grand public (Finlande et Danemark) ainsi qu'en Allemagne et en Autriche. En outre, les acteurs professionnels qui *sont* nés *avec* l'Internet et qui perçoivent sans doute mieux que d'autres les attentes et les exigences des internautes à l'égard des bonnes pratiques sont très majoritairement favorables à la solution du « consentement » (opt in) qui, à leurs yeux, présente un considérable avantage en terme de communication commerciale dans la mesure où, à la différence des registres d'opposition (opt out) qui ne permettent de communiquer qu'à partir de souhaits inexprimés, les listes compilées d'adresses de personnes « consentantes » exprimeraient une « multitude de désirs de consommation et de centres d'intérêts précis » à valeur ajoutée marchande beaucoup plus élevée. C'est en tout cas ce qui résulte de l'étude des pratiques les plus récentes aux Etats-Unis à laquelle a procédé la Commission européenne[8].

Pour sa part, la CNIL souhaite que le débat qui s'engagera sur ce sujet permette d'établir une règle claire, de nature à assurer la confiance et le respect des droits des internautes, alors que les dispositifs arrêtés par plusieurs directives européennes paraissent sur ce point contradictoires. Aussi, convient-il d'en revenir aux principes généraux posés par la directive européenne du 24 octobre 1995 :

— toute collecte de données opérée dans un espace public de l'Internet, sans le consentement des personnes concernées, doit être considérée comme irrégulière et déloyale,

— toute personne (client ou visiteur du site) doit pouvoir s'opposer en ligne à une utilisation commerciale de ses données ou à une cession commerciale

[7] « Communications commerciales non sollicitées et protection des données » — Internal Market DG, octobre 2000.

[8] Rapport déjà cité — Internal Market DG.

des données ainsi collectées à un tiers, à des fins de prospection commerciale.

Une telle manière de voir n'est en rien contraire aux intérêts du commerce électronique puisqu'elle permettrait à tout commerçant en ligne de recourir à la messagerie électronique pour adresser des offres ou propositions nouvelles à l'ensemble de ses clients ou des visiteurs du site, dès lors que ces derniers auraient été préalablement informés, par une mention en ligne, d'une telle éventualité et de leur possibilité de s'y opposer, comme l'exigent d'ailleurs les règles ordinaires de protection des données personnelles et comme le pratique déjà l'ensemble des professionnels dans le monde hors ligne.

Elle permettrait également aux professionnels de céder leurs fichiers de clients ou de prospects, ou d'utiliser le fichier d'un tiers mis à leur disposition, dès lors que les adresses électroniques ainsi utilisées, cédées ou acquises, concerneraient des personnes ayant été préalablement informées de telles cessions ou de tels usages, et de leur droit de s'y opposer.

La solution préconisée par la Commission interdirait en revanche clairement deux pratiques :
la collecte massive (et à l'insu des personnes concernées) d'e-mail dans les espaces publics de l'Internet où l'on peut souhaiter avoir un échange au sein d'une communauté partageant un même sujet d'intérêt sans que son adresse ou ses propos soient immédiatement exploités par un tiers à des fins étrangères au forum ou à la liste de discussion,
la cession de données personnelles collectées par un site A à un tiers lorsque les internautes ayant communiqué leur adresse électronique au site A n'ont pas été informés de l'éventualité d'une telle cession et mis en mesure de s'y opposer, aussitôt et en ligne.

De nombreux organismes de labellisation de sites commerciaux s'engagent déjà à respecter de telles recommandations. Tel est notamment le cas de L@belsite et du Bureau Veritas. On comprend mal que la loi sur la société de l'information ne soit pas mise à profit pour consacrer ces « bonnes pratiques » loin de tout débat, un peu dogmatique, entre le « opt-in » et le « opt-out ».

Aussi, un principe général d'interdiction de collecte des adresses électroniques ou de toute autre donnée personnelle à partir des espaces publics de l'Internet, sans le consentement des internautes, devrait-il être posé par la loi. Toute collecte irrégulière d'adresse électronique dans ces conditions devrait être sanctionnée d'une amende par adresse, une disposition de cette nature paraissant mieux adaptée et plus dissuasive que les dispositions générales de l'article 226-18 du code pénal qui sanctionne la collecte frauduleuse ou déloyale d'une peine de cinq ans d'emprisonnement.

Cette proposition n'exclut nullement la mise en œuvre de registres d'opposition que le projet de loi envisage et dont certains sont déjà mis en oeuvre par des organisations professionnelles. Mais elle leur conférerait, alors, la nature d'ultime « filet de sécurité » qui doit être la leur, comme dans le monde du commerce hors-ligne.

Cette proposition serait conforme au socle de garanties reconnues en la matière par l'ensemble de l'Union européenne et de nature à prévenir les effets du « spamming » en Europe.

L'accès aux données publiques (articles 3 à 6 du projet de loi)

Observations liminaires

Sous un même intitulé le chapitre II du Titre I[er] du projet de loi regroupe des dispositions de nature et de portée différentes : les premières sont principalement destinées à faciliter l'accès du citoyen aux informations détenues par l'Etat ou les collectivités publiques (les données sont alors dites « publiques » parce qu'elles sont collectées ou produites dans le cadre d'une mission de service public) ; les secondes posent un principe général de gratuité et une obligation de mise en ligne sur Internet de l'ensemble des actes et décisions pris dans le cadre d'une mission de service public soumis à une obligation de publicité en vertu de dispositions législatives ou réglementaires (les données sont alors dites « publiques » parce qu'il s'agit de données soumises à un certain régime de publicité).

Une telle présentation ne facilite pas la compréhension des champs d'application (respectifs ou bien se recouvrant pour partie) des deux séries de dispositions.

Le souci d'une plus grande accessibilité de l'information administrative et celui de favoriser les activités économiques liées à la valorisation de l'information administrative ne peuvent qu'être partagés. A cet égard le projet de loi prolonge, à l'heure de la société numérique, la volonté de plus grande transparence que le législateur a manifestée en adoptant la loi au 17 juillet 1978 portant diverses mesures d'améliorations des relations entre l'administration et le public, laquelle a d'ailleurs été modifiée récemment, par une loi du 12 avril 2000, dans le souci de mieux harmoniser ses dispositions avec les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'article 3 du projet de loi n'appellera dès lors que des observations d'ordre juridique et technique.

Tel n'est pas le cas de l'article 4 du projet dont le dispositif d'ensemble, pris dans sa généralité, appelle des observations de fond.

Sur l'obligation de mise en ligne sur Internet de l'ensemble des actes et décisions pris dans le cadre d'une mission de service public, soumis à une obligation de publicité (article 4 du projet)

. Le dispositif prévu

L'article 4 du projet de loi fait obligation à l'ensemble des services de l'Etat et des établissements publics à caractère administratifs de mettre à la disposition du public, sur des sites web accessibles en ligne gratuitement, les données essentielles qui les concernent parmi lesquelles figure « l'ensemble des actes et décisions [...] qui sont soumis à une obligation de publicité en vertu de disposition législative ou réglementaire ».

Un décret en Conseil d'Etat pris après avis de la CNIL « peut » déterminer les actes et les décisions échappant à l'obligation de mise en ligne « en raison des risques particuliers que leur utilisation par des tiers pourrait faire peser sur les libertés individuelles ». Le projet prévoit en outre que la mise en œuvre d'un traitement automatisé de données à caractère personnel préalablement diffusées en ligne est « soumise aux règles posées par la loi du 6 janvier 1978 ».

Il résulte clairement de l'ensemble de ce dispositif que dès lors qu'un acte ou une décision (y compris ceux revêtant un caractère nominatif) sera considéré comme « donnée essentielle », sa mise en ligne obligatoire sera de droit, sauf exception posée par décret en Conseil d'Etat après avis de la CNIL.

Les enjeux

Au regard de la protection des données personnelles et de la vie privée, on peut s'interroger sur le point de savoir si, d'une part, dans la généralité de ses termes, l'obligation qui serait faite de diffuser sur Internet toute donnée « publique », y compris des données personnelles, a suffisamment pris en compte les spécificités liées à un mode de diffusion tel qu'Internet et, d'autre part, si la réserve faite, par exception, pour certains actes et décisions, au motif de risques particuliers que leur utilisation pourrait faire peser sur les libertés individuelles, constitue une garantie suffisante.

En effet, la diffusion d'une information sur Internet réalise un changement d'échelle tout à fait considérable. Toute information diffusée sur Internet devient accessible au plan mondial, et, surtout, les possibilités de duplication et de capture de l'information sont sans limite et ne peuvent être contrôlées. Ainsi, non seulement un site d'information peut être copié à l'infini et stocké sur une multitude de serveurs informatiques sans que le responsable de la diffusion initiale le sache, mais il est également possible, grâce aux prouesses des moteurs de recherche, d'accéder à l'information sans même connaître l'existence du site de diffusion.

Ainsi suffit-il d'indexer le nom d'une personne physique sur un moteur de recherche pour obtenir l'ensemble des informations la concernant diffusées sur Internet à partir de sites géographiquement épars ou de nature différente. Ce qui est techniquement possible lorsqu'une recherche documentaire via Internet est entreprise sur Rabelais, l'est aussi lorsqu'il s'agira de se renseigner sur un candidat à l'emploi ou à un logement, sur un voisin ou un proche, sur un demandeur au crédit, et ce, à l'insu des personnes concernées.

Souligner ces caractéristiques techniques manifeste qu'au-delà des « risques particuliers » qu'une telle diffusion d'informations nominatives est susceptible de présenter au regard des libertés individuelles, et qui justifieraient alors le dispositif d'exception par décret en Conseil d'Etat pris après avis de la CNIL, la diffusion d'une information se rapportant à une personne physique génère un risque « très ordinaire » mais permanent — dès lors qu'il peut suffire d'une diffusion de quelques minutes sur Internet pour générer la duplication et la conservation de l'information en cause, sans limite contrôlable de durée et sur une multitude de serveurs — de réutilisation des informations à l'insu des personnes concernées et étrangère à la finalité de publicité qui a pu, un instant, être recherchée.

Pour n'évoquer que quelques exemples « d'actes ou de décisions pris au nom d'une personne publique qui sont soumis à une obligation de publicité en vertu de dispositions législatives ou réglementaires » et qui devraient, à suivre le projet de loi, être mis en ligne par les administrations ou collectivités publiques concernées, sauf intervention d'un décret dérogatoire en Conseil d'Etat : un jugement portant sur un licenciement pour faute grave, un homicide involontaire, la responsabilité professionnelle d'un praticien, un contentieux fiscal, etc., est naturellement soumis à une obligation de publicité, de même que le rôle des impôts (articles L 104 et L 111 du Livre de procé-

dure fiscale), la liste électorale qui comporte la date de naissance et l'adresse personnelle des personnes (article L 28 du code électoral), les bans de mariages qui comportent la profession et le domicile des futurs époux (article 63 du code civil), le cadastre dont la publicité est organisée par l'article 37 du décret de valeur législative du 7 messidor An II, les permis de construire (article R421-39 du code de l'urbanisme).

Certes, de tels documents sont déjà publics ou communicables aux personnes intéressées.

Mais la publicité jusqu'alors organisée autour de tels actes ou décisions peut poursuivre une finalité particulière ou être assortie de réserves d'usage dont le respect ne pourrait plus être assuré si ces actes et décisions étaient accessibles en ligne. Ainsi la consultation des listes électorales est libre mais il ne peut en être fait une utilisation à des fins exclusivement commerciales, le rôle de l'impôt sur le revenu est consultable à la direction des services fiscaux mais par les seuls contribuables qui relèvent de sa compétence territoriale (le livre des procédures fiscales précisant de surcroît que la publication ou la diffusion par tout autre moyen est interdite sous peine d'amende fiscale), la publicité dont est assortie la délivrance des permis de construire cesse dès la fin du chantier, celle des bans de mariages est exclusivement justifiée par le souci de permettre d'éventuelles oppositions au mariage, celle des décisions de justice par celui de manifester l'impartialité du tribunal et de restituer dans leurs droits toutes les personnes concernées par la décision rendue.

Ces réflexions ne signifient pas qu'il conviendrait pour autant de proscrire toute accessibilité par Internet de telles informations. Ainsi, dans certains cas, la technique peut venir au soutien des précautions à prendre : il pourrait être envisagé, à titre d'exemple, que le cadastre puisse être accessible par Internet dès lors que serait mis en place un système d'accès par cartographie permettant, pour un bien immobilier particulier, d'en connaître le propriétaire. A défaut d'une telle précaution, dont il conviendrait de s'assurer techniquement de l'effectivité, on transformerait un registre de propriétés (à qui appartient cette parcelle que je souhaite acheter ?) en une liste de propriétaires (quels sont les biens que possède Monsieur X ?).

Mais le souci de précaution appelle assurément à un strict encadrement de la diffusion sur Internet d'informations nominatives. Ainsi, le Gouvernement a exclu de la diffusion du Journal officiel sur Internet les décrets de naturalisation afin que la publicité dont sont assortis ces décrets, qui s'apparente à une mesure de bienvenue dans la communauté nationale, ne se transforme pas en menace pesant sur les intéressés, par les possibilités de recherche et de capture de telles informations que peut offrir Internet à certains groupes ou officines de leur pays d'origine. Dans le même esprit, la CNIL mène depuis plusieurs mois une large concertation avec les diffuseurs publics et privés de jurisprudence sur Internet afin d'apprécier les mesures propres à éviter tout détournement de finalité des bases de données des décisions de justice, initialement conçues à des fins exclusives de recherche documentaire, mais qui pourraient se transformer aisément, accessibles gratuitement sur Internet en comportant le nom et quelquefois l'adresse des parties, en véritables bases de renseignements sur les personnes.

En tout état de cause, au-delà de précautions toujours possibles, c'est une certaine retenue dans la diffusion d'informations nominatives qui s'impose, dans le souci de la protection et de la tranquillité des personnes concernées, alors surtout que le projet de loi s'efforce de régler un long contentieux entre

l'Etat et les diffuseurs privés qui ne porte que très marginalement sur des données à caractère nominatif.

L'appréciation de la Commission

Pour l'ensemble de ces motifs la Commission souhaite que, s'agissant des données essentielles revêtant un caractère nominatif, le projet puisse inverser le principe (mise en ligne) et l'exception en limitant l'obligation de mise en ligne des données essentielles aux seuls actes et décisions ne revêtant pas de caractère nominatif, un décret en Conseil d'Etat pris après avis de la CNIL pouvant déterminer ceux des actes et décisions à caractère nominatifs qui pourraient obéir au nouveau régime juridique des « données essentielles ».

Au demeurant une telle suggestion paraît seule conforme aux dispositions de la directive du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données qui n'exclut nullement de son champ d'application les données à caractère personnel revêtant ou ayant revêtu un caractère public, se bornant à ménager quelques exceptions de portée limitée (exception à l'obligation de notification des traitements et exception à l'exigence de subordonner les flux transfrontières de données aux seuls pays disposant d'un niveau de protection adéquat pour les registres qui, en vertu de dispositions législatives ou réglementaires, sont destinés à l'information du public et ouverts à la consultation du public). Ces dérogations n'ont ni pour objet ni pour effet de priver les personnes concernées des droits fondamentaux qu'elles tiennent des législations de protection des données personnelles : droit d'opposition à une utilisation commerciale de données, droit de contrôle de la finalité des traitements mis en oeuvre.

Sur l'obligation de mise à disposition des données numérisées collectées ou produites dans le cadre d'une mission de service public (article 3 du projet)

. Le dispositif prévu

Le projet de loi crée une obligation nouvelle aux personnes publiques et aux personnes privées chargées d'une mission de service public : celle de mettre à la disposition du public les données qu'elles collectent ou qu'elles produisent.

A la différence du dispositif déjà prévu par la loi du 17 juillet 1978 qui, dans son article 10, interdit « la possibilité de reproduire, de diffuser ou d'utiliser à des fins commerciales les documents communiqués », le public (ou les diffuseurs privés) qui pourra accéder à des données sur le fondement de ces dispositions nouvelles, pourra les exploiter pour son propre compte, les utiliser, les diffuser y compris à des fins commerciales, sous réserve de conclure une convention avec la personne ou l'administration détentrice des données, cette mise à disposition pouvant donner lieu à perception d'une redevance. Seront exclues d'une telle mise à disposition les données qui ne sont pas communicables à d'autres personnes que la personne concernée en application de la loi du 17 juillet 1978, modifiée par la loi du 12 avril 2000, soit les données suivantes :

— les documents administratifs dont la consultation ou la communication porterait atteinte au secret des délibérations du Gouvernement et des autorités responsables du pouvoir exécutif, au secret de la défense nationale, à la conduite de la politique extérieure de la France, à la sûreté de l'Etat, à la sé-

curité publique ou à la sécurité des personnes, à la monnaie et au crédit public, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, à la recherche, par les services compétents, des infractions fiscales et douanières, ou, de façon générale, aux secrets protégés par la loi,

— les documents administratifs dont la communication porterait atteinte au secret de la vie privée et des dossiers personnels, au secret médical et au se cret en matière industrielle et commerciale,

— les documents portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ou fai sant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

Le projet de loi précise que la mise à disposition des données à caractère personnel devra s'effectuer dans le respect des règles posées par la loi du 6 janvier 1978.

. Les observations de la Commission

Elles portent principalement sur l'articulation de l'article 3 du projet avec la loi du 17 juillet 1978 modifiée par la loi du 12 avril 2000 et la loi du 6 janvier 1978.

En effet, la loi du 12 avril 2000 avait principalement pour objet de mieux harmoniser les dispositions des deux lois de 1978 dans le souci que l'informatisation de l'administration ne la conduise pas à invoquer la loi « informatique et libertés » pour refuser de communiquer à un tiers un document administratif comportant des informations nominatives, au sens de la loi du 6 janvier 1978, au motif que ce document serait informatisé.

Aussi, suivant en cela les suggestions de la CNIL et du Conseil d'Etat, le législateur a-t-il entendu que l'on ne puisse pas opposer une loi à une autre : le titulaire du droit de communication à l'information administrative est considéré comme un « tiers autorisé » à avoir accès à un traitement, sans que la finalité de ce dernier puisse être opposée à l'exercice de ce droit à la transparence administrative (article 29-1 nouveau de la loi du 6 janvier 1978). Encore convient-il de relever que cet accès ne peut, sur le fondement de ces récentes dispositions, qu'être ponctuel, l'article 10 de la loi du 17 juillet faisant de surcroît interdiction au titulaire du droit de communication de « reproduire, diffuser ou d'utiliser à des fins commerciales les documents ainsi communiqués ».

A cet égard, le projet de loi change la donne puisqu'il paraît ajouter au droit individuel et ponctuel de demander communication d'un document administratif, fut-il numérisé, une obligation générale de mise à disposition de tout document communicable en application de la loi du 17 juillet 1978.

Le problème de coordination entre ces diverses lois serait moins aigu si les informations nominatives étaient exclues du dispositif. Mais, précisément, des informations nominatives peuvent se trouver en cause. Certes, sont considérées comme relevant des exceptions prévues par la loi du 17 juillet 1978 au titre du secret de la vie privée, et à ce titre non communicables à un tiers, la date de naissance, l'âge, la situation familiale, la situation matrimoniale et patrimoniale, l'adresse personnelle, le numéro de téléphone, la formation et les origines professionnelles, le numéro INSEE, les numéros d'immatriculation des véhicules de victimes et de témoins d'accidents.

En revanche, sont communicables, en application de la loi du 17 juillet 1978, l'adresse administrative, l'indice de rémunération, le grade et l'échelon des fonctionnaires et autres agents publics, la liste des commerçants d'une commune avec les montants de la taxe professionnelle acquittée par chacun, la liste des sous-traitants d'un marché public et le montant des interventions effectuées. Aux termes du projet de loi, de tels documents devront désormais être tenus à la disposition du public qui en fait la demande.
Le projet de loi prévoit, certes, qu'une telle mise à disposition devra « s'effectuer dans le respect des règles posées par la loi du 6 janvier 1978 », ce qui constitue une utile garantie dans certaines hypothèses où la CNIL subordonne la diffusion de certaines informations statistiques, particulièrement sensibles mais sur de petits échantillons, pour éviter tout risque de ré-identification des personnes, directement ou indirectement par recoupement.
Mais, le dispositif d'ensemble manque singulièrement de clarté dans la mesure où il prévoit qu'en cas de désaccord entre la personne qui détient les données et celle qui en sollicite la communication, une instance de médiation dont la composition est renvoyée à un décret en Conseil d'Etat pourra être saisie. Or, le projet envisage explicitement que le désaccord puisse porter soit sur la « nature des données communicables », ce qui aurait pu justifier l'intervention exclusive de l'autorité qui est naturellement chargée de porter une appréciation sur ce point (la Commission d'accès aux documents administratifs), soit sur « les modalités d'utilisation ou de diffusion des données », ce qui aurait pu justifier une intervention de la CNIL dans les cas où de telles données revêtiraient directement ou indirectement un caractère nominatif.

La création d'une instance *ad hoc* venant s'ajouter aux deux autorités précédemment citées ne contribue pas à clarifier le dispositif dans son ensemble.

Aussi, tout en partageant pleinement l'objectif général poursuivi par le texte et l'intérêt qui s'attache à mettre à profit les possibilités offertes par la numérisation pour renforcer la transparence administrative et assurer un plus efficace partage de l'information entre l'Etat et les diffuseurs privés, dans le respect de la vie privée des personnes, la Commission ne peut-elle que faire part de sa perplexité sur l'articulation des dispositions de l'article 3 au projet avec celles de la loi du 12 avril 2000.

L'accès aux archives publiques (articles 7 et 8 du projet)

Le dispositif prévu

Le projet de loi réaffirme le principe de libre communication des archives publiques quels que soient leur support, leur lieu, leur mode de conservation et réaménage et, de manière générale, raccourcit les délais spéciaux établis pour certains documents présentant un caractère particulier de confidentialité.

Ainsi, le délai de droit commun de communicabilité de ces documents est ramené de 30 à 25 ans.

Le délai de communicabilité des documents dont la communication porterait atteinte au secret médical et ramené de 150 ans après la naissance à 25 ans après le décès ou, si la date du décès est inconnue, à 125 ans à compter de la naissance.

S'agissant des documents dont la communication porterait atteinte à la protection de la vie privée ou rendrait public une appréciation, un jugement de

valeur ou le comportement d'une personne dans des conditions susceptibles de lui nuire, le délai de libre communication est ramené de 60 à 50 ans à compter de la date du document, ou à 25 ans à compter de la date du décès de l'intéressé. Ces mêmes délais s'appliqueraient aux documents judiciaires. S'agissant des mineurs, l'ensemble de ces délais serait prolongé à 100 ans à compter de la date du document.

S'agissant enfin des délais de communication des registres de l'état civil, le délai de 100 ans est maintenu pour les registres de naissances mais ramené à 50 ans pour les registres de mariages.

Des possibilités de dérogation sont aménagées permettant la consultation des documents protégés avant l'expiration des délais de libre communication lorsque « l'intérêt qui s'attache à la consultation de ces documents ne conduit pas à porter une atteinte disproportionnée aux intérêts que la loi a entendu protéger ». Le bénéficiaire de l'autorisation est alors tenu de ne publier et de ne communiquer aucune information recueillie dans les documents qui soit susceptible de porter atteinte aux intérêts protégés par la loi.

L'appréciation de la Commission

La libéralisation de l'ouverture des archives est considérée comme souhaitable depuis plusieurs années, de nombreux acteurs s'accordant à reconnaître que le dispositif actuel est, au moins dans certains cas, trop restrictif et les dérogations accordées, souvent discrétionnaires. [9]

La Commission croit cependant devoir souligner que l'informatisation des documents versés aux archives, les facilités d'exploitation des informations qu'elle permet et les usages possibles de telles exploitations par des tiers devraient appeler à une certaine prudence, hors le cas où les informations seraient traitées à des fins historiques, statistiques ou scientifiques. Mais précisément ces dernières hypothèses ont déjà conduit à modifier la loi du 6 janvier 1978 en autorisant la conservation des informations nominatives au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été initialement collectées ou traitées et leur traitement à des fins historiques, statistiques ou scientifiques. La loi du 12 avril 2000 a, en effet, modifié à cette fin l'article 28 de la loi « informatique et libertés ». Il résulte, en outre, de cette récente modification législative que tout traitement des données ainsi conservées à des fins autres qu'historiques, statistiques ou scientifiques devra être autorisé, à défaut d'accord exprès des intéressés, par la CNIL ou par décret en Conseil d'Etat sur proposition ou avis conforme de la CNIL.

L'articulation de ces récentes dispositions avec les dispositions du projet de loi soulève deux difficultés.

La première concerne la compatibilité entre un régime de liberté de communication d'archives, une fois les délais de libre communicabilité expirés, et un régime d'autorisation du traitement des données concernées.

La deuxième concerne le sens qu'il convient de donner à la notion de « personnes intéressées ». S'agit-il uniquement des personnes auxquelles les informations nominatives se rapportent ou, le cas échéant, de leurs ayant-droits ?

[9] « Les archives de France » rapport remis par M. Guy Braibant au Premier ministre le 28 mai 1996 — La documentation Française.

Cette question est d'importance.

En effet, s'agissant tout particulièrement des informations dont le projet de loi précise qu'elles seraient susceptibles de porter atteinte à la protection de la vie privée ou de rendre publique le comportement d'une personne dans des conditions susceptibles de lui porter un préjudice ou encore des affaires portées devant des juridictions, les ayant-droits ne disposent-ils pas d'un droit légitime à ce que de telles informations ne puissent être révélées sans garantie pour la mémoire de leurs parents ou leur tranquillité personnelle ? A cet égard une libre communication, 50 ans après l'établissement du document ou 25 ans après le décès de la personne concernée, illustre le caractère pratique d'une telle interrogation.

S'agissant des données médicales, les progrès de la recherche génétique peuvent également donner à penser que la libre communication de telles données 25 ans après le décès de la personne concernée (qui, de surcroît, peut avoir décédé à un jeune âge) n'est pas sans soulever de difficultés. Il pourrait certes être soutenu que le régime d'autorisation aménagé par la loi du 12 avril 2000 pour les traitements de données archivées ne poursuivant pas une finalité historique, scientifique ou statistique est suffisant pour prévenir toute dérive. Cependant, aucune disposition du projet ne subordonne la communication des documents ou des traitements automatisés en cause à la délivrance préalable de cette autorisation de traitement. Que deviendraient de telles données, une fois communiquées à un tiers, si l'autorisation de les traiter n'était finalement pas accordée ?

La Commission croit devoir appeler l'attention sur l'ensemble de ces difficultés.

Il lui apparaît en définitive que les risques particuliers d'atteinte à la vie privée des personnes concernées ou à celle de leurs proches devraient conduire à clairement distinguer les délais et les procédures de communication de documents nominatifs, et plus encore de traitements automatisés de données personnelles, versés aux archives, lorsque la demande de communication ou de traitement de ces informations relève de la recherche historique, scientifique ou statistique.

Dans ces cas, une plus grande libéralisation de l'accès aux archives paraît tout à fait légitime sous la réserve qu'aucune information ainsi recueillie ou traitée puisse être diffusée, traitée ou communiquée à un tiers sous une forme individualisée ou susceptible de porter atteinte aux intérêts protégés par la loi. Seuls la notoriété de la personne en cause, le caractère historique ou public des faits devraient justifier une exception à ce dernier principe.

Dans les autres cas, compte tenu tout à la fois du fait que l'information archivée sera de plus en plus fréquemment numérisée et que les possibilités d'exploitation de cette information par des tiers s'en trouveront accrues (songeons à une diffusion de telles informations sur Internet ou à leur utilisation à des fins marchandes par des compagnies d'assurance, s'agissant des données médicales par exemple, ou bien encore de données à caractère personnel couvertes par le secret statistique), la Commission ne peut qu'émettre des réserves sur le dispositif prévu, sur ce point, par le projet de loi.

Chapitre 2

VIGILANCE AU QUOTIDIEN

I. SPIRITUALITE FORCEE

La CNIL a adopté, le 20 juin 2000, une délibération portant dénonciation au parquet de Paris de l'association spirituelle de l'église de Scientologie d'Ile-de-France pour avoir conservé dans ses fichiers les coordonnées d'une personne qui avait précédemment exercé son droit d'opposition à y figurer.

Déjà en 1998, la CNIL s'était opposée à ce que trois associations satellites de « l'église de Scientologie » constituent un fichier informatique de leurs anciens membres (cf 19e rapport d'activité, p. 14). La CNIL avait estimé qu'en déclarant un fichier d'« anciens membres » n'étant plus en contact avec le mouvement de la Scientologie depuis plus de trois ans, et en indiquant que leurs coordonnées seraient conservées pendant une période supplémentaire de trois ans, ces associations entendaient conserver, sans l'accord des intéressés, des informations nominatives dont elles ne devraient plus disposer et qui auraient dû être radiées. A cette occasion, la Commission avait rappelé « que les informations nominatives concernant les membres d'une association ne peuvent être conservées après leur démission ou leur radiation, sauf accord exprès des intéressés », et que dans ces conditions, la mise en oeuvre de tels fichiers « serait de nature à porter atteinte à la liberté individuelle des personnes concernées ».

La Commission avait alors observé qu'elle était régulièrement saisie de plaintes émanant d'anciens membres ou correspondants de la mouvance « Scientologie » qui, bien que ne le souhaitant plus, continuaient à être destinataires de publications ou de courriers de sollicitation en provenance des associations liées à la Scientologie (l'association spirituelle de l'église de Scientologie d'Ile-de-France, le centre de dianétique, la commission des citoyens pour les droits de l'homme, le Celebrity Center). Les nombreuses demandes de ces particuliers ont dès lors conduit

la CNIL à intervenir systématiquement auprès d'elles pour faire radier les coordonnées de ces personnes de leurs fichiers.

A nouveau saisie par un plaignant, la Commission avait enregistré la décision prise par l'association spirituelle de l'église de Scientologie d'Ile-de-France de radier de ses fichiers les coordonnées de ce requérant. Or, ce dernier a reçu, par la suite, divers documents de cette association dont l'étiquette-adresse informatisée comportait le même numéro d'identification que celle relevée trois ans auparavant.

Aussi la Commission a-t-elle considéré que la conservation et l'utilisation par cette association de Scientologie de ces données, en méconnaissance du droit d'opposition qui avait été exercé, et contrairement aux assurances qui lui avaient été données, constituent des infractions à la loi « Informatique et Libertés » du 6 janvier 1978. La Commission a souhaité porter ces faits à la connaissance de la justice ; cette dénonciation a été jointe à une procédure pénale également ouverte à l'encontre de l'association spirituelle de l'église de Scientologie d'Ile-de-France (ASESIF) à la suite de deux plaintes pour atteinte à la vie privée, qui avaient été déposées directement auprès de la justice.

Délibération n° 00-035 du 20 juin 2000 portant dénonciation au parquet de faits imputés à l'association spirituelle de l'église de Scientologie d'Ile-de-France

La Commission nationale de l'informatique et des libertés,

Saisie par un requérant d'une demande de radiation de ses coordonnées des fichiers détenus par l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France » ;

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 les saisines de la Commission portant les n° 97003571 et 00005238 ;

Vu les courriers adressés par la CNIL à l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France » les 18 septembre 1997 et 10 mai 2000, et les réponses de l'association en date des 2 janvier 1998 et 29 mai 2000 ;

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

Formule les observations suivantes :

Monsieur L. a saisi la Commission nationale de l'informatique et des libertés, le 10 avril 2000, en lui signalant avoir à nouveau reçu à son domicile des courriers émanant de l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France », datés des 30 mars et 6 avril 2000,

alors qu'il avait précédemment demandé la radiation de toute information le concernant des fichiers de cette association.

En effet, en septembre 1997, la CNIL était intervenue à la demande du requérant, auprès l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France », pour obtenir la radiation de ses coordonnées des fichiers et traitements automatisés de l'association. A la suite de cette intervention, l'association en cause avait fait connaître à la CNIL, par un courrier du 2 janvier 1998, que toutes les démarches nécessaires avaient été effectuées, ce dont la CNIL avait informé le requérant.

L'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France », qui ne conteste pas que l'intéressé ait été à nouveau rendu destinataire de courriers les 30 mars et 6 avril 2000, malgré les engagements antérieurement pris, a fait savoir à la CNIL, par un courrier du 29 mai 2000, qu'elle diligentait une « enquête interne pour déterminer les causes de ce dysfonctionnement ».

L'annonce de ces diligences, à supposer même qu'elles soient effectivement menées, laisse entier le fait que les nom et adresse de M. L. ont fait l'objet d'un traitement automatisé d'informations nominatives par l'association dénommée « l'association spirituelle de Scientologie d'Ile-de-France », alors que l'intéressé avait antérieurement exercé son droit d'opposition.

De surcroît, il doit être relevé que les étiquettes-adresses des courriers qui ont été adressés au requérant par divers groupements liés à la « Scientologie » (la Foundation Church of Scientology de Clearwater — USA et la Church of Scientology d'Hollywood — USA en 1997 ; l'association spirituelle de scientoloqie d'Ile-de-France — Paris en 2000) comportent un même numéro à six chiffres, quels que soient l'identité de 'organisme expéditeur et son pays d'établissement, ce qui atteste que l'indexation informatique des coordonnées de M. L. dans la base de données est demeurée inchangée postérieurement à l'exercice de son droit d'opposition et qu'elle est commune à des bases de données situées aux Etats-Unis et à, au moins, une base de données située en France (celle de l'association dénommée « l'association spirituelle de Scientologie d'Ile-de-France »).

Enfin, il est établi que l'information que l'association en cause avait portée à la connaissance de la Commission, par courrier du 2 janvier 1998, selon laquelle il avait été satisfait à la demande de radiation de M. L., était inexacte.

En conséquence,

Décide, en application des dispositions de l'article 21-4° de la loi n° 78-17 du 6 janvier 1978, de dénoncer au Parquet :
d'une part, le fait d'avoir procédé à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, fait imputable à l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France », susceptible de constituer l'infraction visée par l'article 226-18 du code pénal
d'autre part, le fait d'avoir entravé l'action de la CNIL, en lui ayant fait part, dans un courrier du 2 janvier 1998, d'informations inexactes, fait imputable à l'association dénommée « association spirituelle de l'église de Scientologie d'Ile-de-France », constitutif de l'infraction visée par l'article 43 de la loi du 6 janvier 1978.

II. DEFENSE DU LOGEMENT SOCIAL

Dans son rapport publié en décembre 1998, le Haut Conseil à l'intégration rappelait les résultats d'une enquête statistique menée conjointement par l'INED et l'INSEE en 1992 : alors que la moyenne nationale des personnes logées en « HLM dégradés » était de 3 %, le pourcentage s'élevait à 17 % pour les familles originaires d'Algérie et du Maroc, à 18 % pour les ressortissants turcs et à 12 % pour les personnes originaires d'Afrique noire. Il était relevé, s'agissant de ces dernières, que le pourcentage des familles occupant un logement dans le « parc privé dégradé » s'élevait à 16 % alors que la moyenne des ménages y résidant est de 2 %.

Peu de temps auparavant le législateur, dans la loi du 29 juillet 1998 relative à la lutte contre les exclusions, avait fait référence, à différentes reprises, à la notion de mixité sociale qui a été introduite dans le code de la construction et de l'habitation. Ainsi, dans l'article premier de ce texte, il est indiqué que « la lutte contre les exclusions est un impératif national fondé sur le respect de l'égale dignité de tous les êtres humains », et que afin de « garantir sur l'ensemble du territoire l'accès effectif de tous aux droits fondamentaux dans les domaines de l'emploi, du logement », l'Etat, les collectivités territoriales, les établissements publics dont les centres communaux et intercommunaux d'action sociale doivent y participer.

Dans le souci de promouvoir ou d'assurer la « mixité sociale », la CNIL a admis, en matière de logement social, que la nationalité des locataires puisse être collectée et traitée informatiquement par les bailleurs sociaux, dans le double but d'éviter la constitution de « ghettos », et fout particulièrement de « ghettos ethniques », et de s'assurer du respect des dispositions relatives à la contribution patronale à l'effort de construction réservée au logement des immigrés prévue par une circulaire interministérielle du 20 juillet 1976. Précédemment, la CNIL, par une délibération 97-005 du 21 janvier 1997, avait considéré que l'information relative à la nationalité peut être connue des organismes participant à la décision d'attribution des logements, et également des maires des communes conformément aux dispositions de la loi d'orientation de la ville du 13 juillet 1991, dont la finalité était « de favoriser la cohésion sociale de nature à éviter ou à faire disparaître les phénomènes de ségrégation ».

Plusieurs réclamations adressées depuis lors à la Commission laissent à penser que cet objectif n'a pas été atteint : on peut en trouver confirmation dans la démarche de l'Union nationale des HLM qui a demandé à trois personnalités (Madame Simone Veil, Madame Nicole Questiaux et Monsieur Paul Bouchet) de lui présenter des propositions en la matière.

Le risque existe, il est vrai, qu'à partir de l'exploitation des données collectées auprès des demandeurs ou des occupants de logements sociaux, dans les fichiers informatiques mis en œuvre par les organismes de logements sociaux — qu'ils soient publics ou privés —, qu'une « discrimination instantanée » n'apparaisse pas immédiatement légitime aux intéressés ou pertinente. Un doute peut naître sur un éventuel risque de discrimination que l'ordinateur pourrait favoriser.

C'est eu égard à ce danger que la CNIL recommande de ne recueillir l'information relative à la nationalité des personnes que sous la forme « Français — Union européenne — Etrangers hors Union européenne » et s'oppose à la diffusion de résultats statistiques agrégés à un niveau géographique ou de population trop faible, lorsque les informations en cause concernent la nationalité, le mode d'acquisition de la nationalité française ou encore les origines géographiques, c'est-à-dire le plus souvent le lieu de naissance des parents. Elle fait également preuve d'une grande vigilance s'agissant des méthodes d'analyses statistiques, dénommées « ilôtypage négatif » qui consistent, à partir de recoupement d'informations (issues notamment de l'INSEE, de bases de données de « marketing », du taux de recouvrement d'impayés, de la proportion de populations étrangères ou de familles mono parentales ou encore de Rmistes), à caractériser non pas le « profil » d'une personne, mais celui d'un territoire (l'ilôt) dont les caractéristiques seront supposées être celles du groupe, considéré comme homogène. L'ilôt, unité statistique de base, correspond généralement à une zone de peuplement considérée comme homogène de l'ordre de 150 habitants.

Lorsqu'il s'agit d'utiliser de tels systèmes d'informations géographiques pour limiter la prospection commerciale aux seuls quartiers supposés correspondre à la « cible commerciale » du produit, aucun risque n'est à redouter. Or ce qui est recherché, c'est non de sélectionner une cible commerciale mais d'exclure toutes les personnes d'un même « ilôt » considéré comme étant à risque, c'est-à-dire de prendre une décision non pas en fonction de la personne mais exclusivement en fonction de son adresse.

Ce « profilage » du territoire et le risque de discrimination qu'il pourrait susciter expliquent la vigilance dont il convient de faire preuve en matière de collecte et de traitement de l'information dans le domaine du logement social.

Aussi la CNIL a-t-elle pour politique de procéder systématiquement à des contrôles ou des vérifications sur place chaque fois qu'elle est saisie d'une plainte ou d'une réclamation mettant en cause la légitimité de la collecte ou du traitement d'une information pouvant donner à penser aux personnes accueillies dans la communauté française ou à celles qui sont de nationalité française qu'elles font l'objet d'une discrimination en fonction de leurs « origines » supposées. Elle constate que l'interrogation sur la nationalité, loin de contribuer à la mixité sociale exigée par le législateur, peut avoir comme conséquence une « ghettoïsation » en matière d'attribution de logements. Rien ne serait pire qu'un idéal proclamé d'universalité de la citoyenneté et de mixité sociale, si, dans les faits, l'attention des organismes bailleurs à préserver une certaine forme de « tranquillité », et/ou la pression « sociale » ou celle de certains « présupposés », conduisaient en définitive à répartir le territoire en fonction de soit-disant « communautés ethniques ».

A. Le contrôle d'une société HLM à la Rochelle

La Commission a contrôlé la société anonyme d'HLM, « le Foyer de la Charente maritime », située à la Rochelle, accusée en 1998 de recourir pour la sélection

des demandeurs de logement à un système de score sur la base de fiches renseignées indirectement par les candidats à un logement et de constituer un fichier de personnes fragilisées. A cette époque, la Commission était intervenue fermement pour rappeler à l'organisme en cause sa doctrine constante sur la constitution de fichiers de personnes « à risques » et sur les traitements automatisés donnant une définition d'un profil. La Commission avait tout particulièrement estimé que la mise en place d'une grille de « score » dont l'attribution des points aboutissait à infliger aux familles particulièrement fragiles une notation très faible affectait d'illégalité la procédure d'attribution.

La Commission a en outre procédé à une mission de contrôle sur place pour vérifier la régularisation de la situation. Elle a constaté que les engagements pris par le président de l'organisme qui avait indiqué que ces pratiques litigieuses avaient été mises en place par un de ses collaborateurs et à son insu, avaient été tenus :

— les fiches litigieuses collectées à l'insu du conseil d'administration avaient été détruites et aucune exploitation informatique n'avait été réalisée ; il faut rappeler que ces fiches contenaient des informations dépourvues de toute pertinence dans le processus d'attribution de logements, notamment la possession d'un véhicule à moteur, le niveau de formation ou encore le nombre de ruptures familiales ;

— le fichier des personnes fragilisées comportant l'enregistrement des locataires ayant bénéficié d'une aide sociale, avait été détruit ;

— il n'existait pas de système de scoring.

B. Le contrôle de la SOGINORPA à Douai

La SOGINORPA, premier propriétaire bailleur de la région Nord-Pas-de-Calais, gère un patrimoine de 70 000 logements initialement construits par les compagnies minières pour y loger gratuitement leur personnel. Aujourd'hui encore, et malgré l'ouverture depuis 1970 du parc de la SOGINORPA au marché locatif, ce patrimoine est occupé majoritairement par les « ayants droit » des ouvriers mineurs.

La CNIL a effectué un contrôle, le 1er mars 2000, au siège de cet organisme bailleur social, à Douai, après avoir été saisie, en fin d'année 1999, de réclamations émanant d'associations de lutte contre le racisme (SOS Racisme, Mouvement contre le racisme et pour l'amitié entre les peuples) et d'un particulier, à propos de la collecte, par la SOGINORPA, de « l'origine » de ses locataires ainsi que de celle des membres de leur foyer. Un questionnaire, visant notamment à recueillir « l'origine » des intéressés sous la forme « français, européen non-français, non-européen », avait été diffusé aux occupants des immeubles. Enfin, un jeu-concours organisé par le bailleur permettait en outre aux locataires ayant répondu à l'enquête de participer à un tirage au sort dont le premier prix était un voyage.

La Commission a exigé de la SOGINORPA qu'elle supprime « dans les plus brefs délais » cette donnée de ses fichiers dès lors que, « si la nationalité est une information qui peut éventuellement être utile aux bailleurs sociaux et paraît susceptible, le cas échéant, d'être recueillie en vertu des textes en vigueur et de la norme

simplifiés n° 20, l'origine des intéressés ne permet aucunement de répondre aux critères d'attribution ou de gestion des logements sociaux ».

En réponse, le directeur général de l'organisme incriminé s'excusant pour « l'erreur commise » dans la terminologie employée affirmait que son seul objectif était de recueillir la nationalité des intéressés. Il s'engageait par ailleurs :
à détruire, sous le contrôle d'un huissier, toute information éventuellement retrans crite dans les fichiers de la société sous le libellé « origine » ;
à mettre sous scellés l'ensemble des questionnaires papier, la levée des scellés par huissier n'étant opérée que pour procéder au tirage au sort des gagnants, confor mément au jeu organisé avec l'envoi des questionnaires ;
à détruire devant huissier l'ensemble des questionnaires, après la réalisation du tirage au sort ;
à adresser un rectificatif aux occupants afin de lever toute ambiguïté sur les moti vations de cette collecte et de les informer des prescriptions de l'article *17* de la loi du 6 janvier 1978 leur donnant la possibilité de faire procéder à toute correction ou sup pression des informations les concernant qui auraient pu être recueillies à l'occasion de cette enquête.

Lors de sa mission de contrôle, la CNIL s'est s'assurée du respect des engagements de la SOGINORPA, et a pu faire le point sur les informations nominatives nécessaires aux bailleurs tant dans la procédure d'attribution que dans la gestion des logements sociaux. La Commission s'est aussi fait préciser les informations collectées sur les candidats à la location en vue de respecter le principe de mixité sociale.

A cet égard, le directeur général de la SOGINORPA a remis à la délégation de la CNIL un document définissant la politique d'attribution de son organisme. Parmi les critères généraux d'attribution, figure la recherche de l'« adéquation entre le type de logement et le demandeur, les ressources, la composition de la famille, le montant du loyer, les charges, le maintien des grands équilibres sociologiques propres à favoriser la quiétude et la qualité de vie dans les quartiers miniers ». Le chômage, la mutation professionnelle, le nombre de personnes à charge, les départs et décès des mineurs retraités ou ayants droit, descendants et collatéraux constituent des éléments prioritaires au regard de l'attribution d'un logement. Enfin, la SOGINORPA indique le caractère essentiel du recueil des revenus aux fins d'assurer la mixité sociale prévue par les dispositions légales.

Par ailleurs, la CNIL a vérifié le système informatique de la société TMT, située à Fontenay-Sous-bois, mentionnée par la SOGINORPA comme « service chargé de la mise en oeuvre du traitement ». Cette mission de vérification lui a permis de prendre acte du fait que l'information litigieuse relative à « l'origine » des personnes était absente des fichiers détenus tant par la SOGINORPA que par son sous-traitant. Toutefois, la Commission a, à cette occasion, rappelé que le remplacement de l'information relative à la nationalité des locataires en place par la mention « IND », ne saurait justifier la déduction de « l'origine » des intéressés grâce à la consonance du patronyme conformément à la recommandation de la CNIL du 11 décembre 1996. Enfin, il a été rappelé que la conservation des informations communiquées par les personnes s'étant portées candidates à l'attribution d'un logement ne peut excéder

un an après la demande ou son renouvellement ainsi que cela est précisé sur le questionnaire de demande de logement.

C. Le contrôle de l'OPAC de Metz

En mai 2000, la CNIL a été saisie par l'association SOS Racisme d'une réclamation relative à la diffusion par l'OPAC de Metz d'un questionnaire destiné à ses locataires désireux de procéder à un échange de logement. Ce document comportait après les rubriques « date et lieu de naissance » et « nationalité », une question relative au « pays d'origine » des intéressés. Une telle information étant tout à fait excessive et non pertinente en matière de fichier de gestion locative, et en aucun cas autorisée par la CNIL, une mission de vérification sur place auprès de l'organisme concerné a été effectuée le 14 juin 2000.

L'OPAC de Metz gère 12 000 logements sociaux, dont 1 400 sont mis en location chaque année : les deux tiers étant attribués à des personnes dites « extérieures » (non déjà logées dans le parc HLM de l'office) et un tiers faisant l'objet d'échanges au sein des locataires en place. Les candidats à la location ou à l'échange d'un appartement sont reçus par des « conseillers clientèle » qui établissent un dossier sur la base des formulaires à remplir par chaque demandeur.

La délégation de la Commission a reçu l'assurance que les candidats sélectionnés et classés en ordre de priorité sont présentés à la commission d'attribution des logements, composée essentiellement d'élus locaux, à laquelle sont communiquées par l'office des informations sur les revenus et la composition de la famille et sur le classement au regard des critères de priorité à l'exclusion de toute donnée relative à la nationalité ou au lieu de naissance des intéressés.

Les représentants de l'OPAC ont invoqué une « erreur matérielle » intervenue à l'occasion de la mise à jour des formulaires de l'office en 1997, tandis que le directeur général a précisé que le personnel de l'OPAC n'inscrivait sous cette rubrique que le « pays de naissance », dont la collecte est prévue par la norme simplifiée n° 20, au titre du « lieu de naissance ». Sur ce point, la CNIL a rappelé que le « lieu de naissance », mentionné au titre des informations pouvant être collectées dans les traitements de gestion de patrimoine immobilier déclarés par le biais de la norme simplifiée n° 20, doit être entendu comme un élément constitutif de l'état civil des personnes physiques, à savoir la ville dans laquelle la naissance a été déclarée pour les personnes nées en France (l'arrondissement pour les personnes nées à Paris, Lyon et Marseille) et la ville ou le cas échéant le pays, s'agissant des personnes nées à l'étranger, étant observé que cette information ne saurait être utilisée à des fins discriminatoires par les bailleurs. Par ailleurs, il a été précisé à la Commission que l'information relative au « pays d'origine » n'avait pas été portée à la connaissance de tiers.

A la suite de cette intervention, le questionnaire litigieux a été modifié afin de supprimer la rubrique « pays d'origine » ; désormais, aucun champ de saisie de l'application informatique ne permet le recueil de cette information. Enfin, la Commission a demandé qu'à l'avenir, les questionnaires de collecte soumis aux

candidats à la location d'un bien immobilier ou aux locataires en place soient complétés par les prescriptions de l'article *17* de la loi en vue d'informer clairement les personnes interrogées du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires des informations, du droit d'accès et de rectification pour les informations les concernant.

En outre, la CNIL est intervenue auprès du concepteur du logiciel pour que cette rubrique, dépourvue de toute pertinence, soit supprimée.

Ces diverses interventions dans le domaine du logement social illustrent la sensibilité particulière du sujet et les préoccupations légitimes des personnes concernées. Sans doute, au regard de l'objectif de mixité sociale, la question se pose de savoir s'il n'y a pas lieu de réévaluer la pertinence et les incidences possibles de la collecte et du traitement des informations relatives à la nationalité des intéressés dans l'attribution et la gestion des logements sociaux. Faut-il préférer que les logements soient attribués sans tenir compte de la nationalité, c'est-à-dire un peu « à l'aveugle » pour éviter les dérives ou les risques d'incompréhension, délétères pour le lien social ? Cette information est-elle déterminante pour assurer la « mixité sociale » ? Convient-il d'admettre, alors que jusqu'à présent la Commission y a toujours été réticente, la collecte de l'information relative aux immigrés « nouveaux arrivants » pour le motif que l'insertion sociale de ceux-ci nécessite une attention particulière ? Et si la nationalité est conservée comme élément pour l'attribution du logement, faut-il par là conserver cette information dans les fichiers de gestion ? Et à quelles fins ?

La Commission a souhaité mener une étude d'ensemble sur ces sujets, en liaison avec tous les partenaires concernés, sensible au fait que la mixité sociale est d'abord une exigence républicaine dont il apparaît qu'elle n'est pas aujourd'hui convenablement satisfaite.

III. MALADIES A DECLARATION OBLIGATOIRE SOUS SURVEILLANCE

A la suite de l'annulation par le Conseil d'Etat, le 30 juin 2000, des dispositions du premier alinéa de l'article R 11 -2 du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire, la direction générale de la santé a saisi la CNIL pour avis d'une nouvelle rédaction de ce texte.

Aux termes des dispositions annulées, il était prévu que « ... la notification des données individuelles est réalisée sous la forme d'une fiche qui comporte des éléments à caractère nominatif et des informations nécessaires à l'épidémiologie, fixés pour chaque maladie, par arrêté du ministre chargé de la santé, sous réserve de l'application des dispositions de l'article 15 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

La Ligue des droits de l'homme qui s'était élevée au cours de l'été 1999 contre les risques d'un « fichage » nominatif des personnes séropositives rendus à ses yeux possible par les termes employés dans le décret du 6 mai 1999, avait saisi le Conseil d'Etat d'un recours en annulation du décret au motif d'une part que la CNIL n'avait pas été saisie du projet de décret et d'autre part, que les dispositions de l'article R 11-2 ne permettaient pas de préserver l'anonymat des personnes séropositives tel que défini par l'article L 3113-1 du code de la santé publique (anciennement L 11). [10]

Le premier moyen a été écarté par la Haute Assemblée au motif que les articles 20 et 28 de la directive européenne du 24 octobre 1995 n'imposaient pas au gouvernement de soumettre préalablement à l'autorité de contrôle un tel texte dès lors qu'il était prévu une consultation de la CNIL sur les projets d'arrêtés créant les traitements.

Sur le second moyen, le Conseil d'Etat a estimé que le gouvernement ne pouvait se décharger légalement de la mission qui lui avait été confiée par le législateur en se bornant à renvoyer purement et simplement à un arrêté ministériel le soin de déterminer, fût-ce après avis de la CNIL, les règles concernant le respect de l'anonymat.

Le nouveau projet examiné par la Commission au cours de sa séance du 3 octobre 2000 précise le contenu, les modalités d'établissement et de transmission des déclarations obligatoires de certaines maladies selon deux modes de surveillance prévus à l'article R 11-1 du code de la santé publique : les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique et qui imposent la transmission de données « individuelles » à l'autorité sanitaire, et les maladies qui nécessitent une intervention urgente locale, nationale ou internationale.

Dans sa délibération n° 00-45 du 3 octobre 2000, la Commission a tout d'abord souhaité rappeler les principes qui doivent commander la mise en place des procédures de déclaration obligatoire de certaines maladies et qu'elle avait énoncés dans sa délibération du 9 décembre 1999 portant adoption du rapport relatif aux modalités d'informatisation de la surveillance épidémiologique du sida — à propos de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine[11].

Ainsi, les centres de dépistage anonymes et gratuits (CDAG) doivent être exclus du dispositif, l'instauration d'une déclaration obligatoire fondée sur l'identification même indirecte de la personne, et fut-elle codée, étant de nature à dissuader les personnes de se faire dépister dans ces centres.

De même, tout en relevant avec satisfaction que le projet de décret prévoyait la mise en place d'un dispositif d'anonymisation à la source des éléments d'identification de la personne par une technique de codage dite « irréversible », la Commission a considéré que le texte devait énumérer la nature des données individuelles

[10] Cf 20e rapport d'activité de la CNIL.
[11] Cf 20e rapport d'activité.

appelées à être portées sur la fiche de notification et parmi celles-ci, celles susceptibles de faire l'objet d'un chiffrement. De surcroît, dans le souci qu'aucune réidentification des personnes ne soit possible et que l'anonymat soit parfaitement assuré, la CNIL a recommandé que « au titre du lieu de domicile, seul le département de domicile de la personne soit collecté à l'exclusion du code postal et que, s'agissant de la profession de la personne, seule la catégorie professionnelle, telle qu'elle résulte de la classification à deux chiffres de l'INSEE soit retenue et non la profession précise des personnes ».

La CNIL a également souhaité que le texte soit complété d'une mention spécifique sur la nécessaire confidentialité qui doit entourer la conservation par le médecin déclarant de la table de correspondance entre le numéro de code et l'identification de la personne.

Par ailleurs, la CNIL a estimé, s'agissant du contenu des déclarations obligatoires, que le maintien des termes « éléments à caractère nominatif » était de nature à entretenir la confusion avec les dispositions de la loi qui évoque, elle, l'anonymat.

En outre, la Commission a considéré surabondante et comme devant être supprimée la mention dans le décret des sanctions pénales encourues en cas d'absence de protection, de détournement des informations recueillies et d'atteinte au secret de la correspondance ou aux systèmes de traitement automatisé de données.

Enfin, la CNIL a estimé que le texte du décret devait être complété d'un article spécifique destiné à autoriser, conformément aux dispositions de l'article 31 de la loi du 6 janvier 1978, l'enregistrement et la conservation des données à caractère personnel relatives aux pratiques sexuelles des personnes, puisque la connaissance de telles données (anonymisées) n'est pas sans utilité pour la recherche épidémiologique.

Le décret du 16 mai 2001 — paru au JO du 23 mai 2001 — reprend la plupart des observations formulées par la CNIL.

Délibération n° 00-045 du 3 octobre 2000 portant avis sur un projet de décret modifiant les articles R 11-1, R 11-2, R 11-3 et R 11-4 du code de la santé publique issus du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuell es concernant les maladies à déclaration obligatoire

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le directeur général de la santé d'un projet de décret modifiant les articles R 11-1, R 11-2, R 11-3 et R 11-4 du code de la santé publique issus du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire ;

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 le décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies visées à l'article L 11 du code de la santé publique ;

Vu le décret n° 99-363 du 6 mai 1999 fixant la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire et modifiant le code de la santé publique ;

Après avoir entendu Monsieur André Bohl en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations

Formule les observations suivantes :

Le ministère de l'Emploi et de la Solidarité a saisi la Commission, pour avis, d'un projet de décret visant à modifier les articles R 11-1, R 11-2, R 11-3 et R 11-4 du code de la santé publique issus du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire visées à l'article L 3113-1 du code de la santé publique — anciennement article L 11 —.

La présentation de ce nouveau texte fait suite à l'annulation par le Conseil d'Etat du premier alinéa de l'article R 11-2 du décret n° 99-362 du 9 mai 1999, aux termes duquel : « la notification des données individuelles est réalisée sous la forme d'une fiche qui comporte des éléments à caractère nominatif et des informations nécessaires à l'épidémiologie, fixés, pour chaque maladie, par arrêté du ministre chargé de la santé, sous réserve de l'application des dispositions de l'article 15 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

Le Conseil d'Etat a en effet estimé que « ... s'il appartenait éventuellement au gouvernement, après avoir défini avec une précision suffisante dans le décret en Conseil d'Etat les principes qu'il entendait retenir pour protéger, comme le lui demandait le législateur, l'anonymat des personnes dont les données individuelles sont ainsi recueillies, de renvoyer à un arrêté ultérieur le soin de préciser, en tenant compte éventuellement de la nature de la maladie ou de l'objectif poursuivi par la collecte, les modalités de l'application de ces principes, il ne pouvait se décharger légalement de la mission que lui avait confiée l'article L 11 précité en se bornant à renvoyer purement et simplement à un arrêté ministériel le soin de déterminer les règles concernant l'objet ci-dessus défini ».

Le nouveau projet de décret a pour objet de décrire le contenu, les modalités d'établissement et de transmission des déclarations obligatoires de certaines maladies selon les deux modes de surveillance prévus à l'article R 11-1 du code de la santé publique. Sont ainsi distinguées les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique et qui imposent la transmission de données individuelles à l'autorité sanitaire et les maladies qui, nécessitant une intervention urgente locale, nationale ou internationale, peuvent également conduire à communiquer, sur demande des médecins inspecteurs de santé publique, le nom et l'adresse de la personne.

Sur les garanties devant être reconnues aux personnes :

Saisie de ce nouveau texte, la Commission rappelle les principes qui doivent commander la mise en place des procédures de déclaration obligatoire de certaines maladies et qu'elle a énoncés dans sa délibération du 9 décembre 1999 portant adoption du rapport relatif aux modalités d'informatisation de la surveillance épidémiologique du sida — à propos de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine. Afin de garantir l'anonymat des déclarations lors de leur transmission à l'autorité sanitaire, un système dit « d'anonymisation » à la source des déclarations à l'aide d'un codage informatique des initiales des nom et prénom et de la date de naissance doit être mis en place. L'identification du lieu de domicile de la personne doit être limitée au département et, seule la catégorie socio-professionnelle doit être recueillie.

Les pouvoirs publics doivent s'assurer des mesures nécessaires pour garantir au niveau départemental la confidentialité des déclarations adressées aux médecins inspecteurs des directions départementales des affaires sanitaires et sociales (DDASS), telle que la destruction des supports papier une fois les informations transmises à l'Institut de la veille sanitaire

S'agissant des déclarations des cas d'infection par le virus de l'immunodéficience humaine, les centres de dépistage anonymes et gratuits (CDAG) doivent être exclus du dispositif, l'instauration d'une déclaration obligatoire fondée sur l'identification même indirecte de la personne, et fut-elle codée, étant de nature à dissuader les personnes de se faire dépister dans ces centres.

Sur le contenu des déclarations obligatoires (1er, 2e, 3e et 4e alinéas de l'article R 11-2) ;

La Commission relève en premier lieu que sont maintenus au premier alinéa de l'article R 11-2 du projet de décret (es termes « éléments à caractère nominatif ». Or, dans la mesure où les dispositions de l'article L 3113-1 du code de la santé publique prévoient que les modalités de transmission à l'autorité sanitaire, fixées par décret en Conseil d'Etat, doivent garantir l'anonymat des personnes concernées et où les dispositions du projet de décret ont précisément pour objet de fixer le contenu de la fiche de notification et de prescrire une procédure d'anonymisation à la source des données d'identification, l'expression d'« éléments à caractère nominatif » est susceptible de susciter la confusion et devrait être évitée.

Ainsi, le deuxième alinéa de l'article R 11-2 prévoit que pour les maladies inscrites sur la liste fixée à l'article D 11-2 (c'est-à-dire nécessitant une intervention urgente), la fiche ne comporte que les éléments d'identification « strictement nécessaires pour garantir la qualité du recueil d'informations, à l'exclusion du nom patronymique complet et de tout autre numéro d'identification créé à d'autres fins. Ces éléments peuvent être rendus anonymes à la source par technique de codage irréversible ».

Le troisième alinéa de l'article R 11-2 précise, pour les maladies inscrites sur la liste fixée à l'article D 11-1 (c'est-à-dire nécessitant une surveillance à des fins d'évaluation de la politique de santé) que « le déclarant rend anonyme à la source les éléments d'identification par technique de codage irréversible. La correspondance établie par le médecin déclarant entre le numéro de code et les éléments d'identification de la personne, aux fins de valida-

tion et d'exercice du droit d'accès, est détruite six mois après la date de notification portée sur la fiche ».

La Commission relève ainsi que le décret prévoit désormais la mise en place d'un dispositif d'anonymisation à la source des éléments d'identification de la personne par technique de codage irréversible ainsi qu'elle l'avait recommandé dans sa délibération du 9 décembre 1999.

La Commission estime toutefois que le projet de décret devrait énumérer limitativement, au moins pour les maladies inscrites sur la liste fixée à l'article D 11-1 du code de la santé publique, les données individuelles qui pourront être portées sur la fiche de notification. Tout en prenant acte que ces données seront chiffrées par un algorithme irréversible, la CNIL rappelle qu'elle avait souhaité que seules les initiales du nom et du prénom de la personne soient collectées ainsi que la date de naissance ; qu'au titre du lieu de domicile, seul le département de domicile de la personne soit collecté à l'exclusion du code postal et que, s'agissant de la profession de la personne, seule la catégorie professionnelle, telle qu'elle résulte de la classification à deux chiffres de l'INSEE soit retenue et non la profession précise des personnes.

Si pour les déclarations des maladies dont la surveillance épidémiologique est nécessaire pour évaluer les politiques de santé, la mise en place d'un dispositif d'anonymisation des données d'identification par codage à la source est imposé, le deuxième alinéa de l'article R 11 -2 prévoit que pour les maladies nécessitant une intervention urgente, le recours à un tel dispositif n'est pas obligatoire. En effet, il est nécessaire pour ces maladies de pouvoir, le cas échéant, contacter le patient pour entreprendre une action de prévention.

La Commission estime toutefois que les cas dans lesquels ce dispositif d'anonymisation serait susceptible de ne pas s'appliquer devraient être précisés. Il est également prévu au troisième alinéa de l'article R 11-2 qu'une liste de correspondance est établie par le médecin déclarant entre le numéro de code et les éléments d'identification de la personne aux fins de validation et d'exercice du droit d'accès. Cette liste est conservée six mois.

La Commission estime nécessaire de compléter l'alinéa précité d'une mention sur les conditions particulières de confidentialité qui doivent entourer cette liste de correspondance.

La Commission relève qu'aux termes de l'alinéa quatre de l'article R 11-2 : « Un arrêté du ministre chargé de la santé fixe, pour chaque maladie, les critères cliniques et biologiques de la notification ainsi que les données figurant sur la fiche, après avis de la Commission nationale de l'informatique et des libertés ».

Sur les modalités de transmission des déclarations obligatoires (5e, 6e et 7e alinéas de l'article R 11-2) :

Le 5e alinéa de l'article R 11-2 du projet de décret prévoit que le déclarant transmet la fiche, soit par voie postale sous pli confidentiel portant la mention secret médical, soit par télétransmission après chiffrement des données, au médecin inspecteur de santé publique de la direction départementale des affaires sanitaires et sociales ou au médecin désigné par arrêté du préfet du département.

Le 6e alinéa de l'article R 11 -2 prévoit que le médecin destinataire rend anonymes les éléments d'identité par technique de codage irréversible. La cor-

respondance qu'il établit entre le numéro de code et les éléments d'identification de la personne, aux fins de validation et d'exercice du droit d'accès, est détruite six mois après la date de notification portée sur la fiche.

Le 7e alinéa de l'article R 11-2 précise les modalités de transmission des déclarations obligatoires au médecin de l'Institut de veille sanitaire désigné par son directeur général.

Ces dispositions n'appellent pas d'observation particulière de la part de la Commission.

Sur l'article R 11-4 :

Le premier alinéa de l'article R 11-4 rappelle que les personnes appelées à connaître à quelque titre que ce soit, les données individuelles transmises en application des articles R 11-2 et R 11-3 « sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal ». Le projet de décret complète ces dispositions par deux alinéas énumérant les sanctions pénales encourues en cas « d'absence de protection » et de « détournement des informations recueillies » dans le cadre des procédures décrites à l'article R 11-3 et « d'atteinte au secret de la correspondance ou aux systèmes de traitement automatisé de données commise dans le cadre des procédures prévues aux articles R 11-2 et R 11-3.

La Commission considère que l'ajout auquel procède le projet de décret, surabondant, devrait être supprimé.

Sur l'enregistrement de données relatives aux mœurs sexuelles des personnes :

Pour les maladies soumises à déclaration obligatoire et dont un des modes de transmission est de nature sexuelle, les fiches de notification peuvent comporter, à des fins d'exploitation épidémiologique, des informations révélant les pratiques sexuelles des personnes.

L'enregistrement de ces données présente un intérêt de santé publique important.

Dès lors, la Commission estime qu'il y a lieu de proposer l'insertion, dans le présent projet de décret d'une disposition visant à autoriser, conformément aux dispositions de l'article 31 de la loi du 6 janvier 1978, l'enregistrement et la conservation des données à caractère personnel relatives aux pratiques sexuelles des personnes.

Compte tenu de ces observations, la commission émet l'avis suivant :

1) Les deux premières phrases du premier alinéa de l'article R 11 -2 nouveau devraient être supprimées et remplacées par la rédaction suivante : « La notification des données nécessaires à l'épidémiologie est réalisée sous la forme d'une fiche établie et transmise par le médecin qui a fait le diagnostic du cas de la maladie ou par le responsable du service de biologie ou du laboratoire d'analyses de biologie médicale, public ou privé, qui a constaté l'anomalie biologique correspondant à la maladie ».

2) Le troisième alinéa de l'article R 11-2 nouveau devrait être ainsi rédigé : « Pour les maladies uniquement inscrites sur la liste fixée à l'article D 11-1, la fiche comporte les éléments d'identification suivants : un numéro de code établi par technique de codage irréversible à partir des initiales du nom, du

prénom et de la date de naissance, le département de domicile et la catégorie socio-professionnelle de la personne. La correspondance établie par le médecin déclarant entre le numéro de code et les éléments d'identification de la personne, aux fins de validation et d'exercice du droit d'accès, est conservée dans des conditions garantissant la confidentialité des informations et détruite six mois après la date de notification portée sur la fiche ».

3) Le paragraphe IV de l'article premier du projet de décret devrait être sup primé.

4) Le projet de décret devrait être complété d'un article R 11 -5 ainsi rédigé : « Pour les maladies visées à l'article R 11-2 et dont un des modes de trans mission est de nature sexuelle, les médecins déclarants, les médecins inspec teurs visés à l'article R 11-2 et les médecins de l'Institut de veille sanitaire visés à l'article R 11-2 sont autorisés à enregistrer et conserver, dans les conditions définies aux articles R 11-2 et R 11-3, des données à caractère personnel qui, étant relatives aux pratiques sexuelles des personnes, relè vent des données visées par l'article 31 de la loi du 6 janvier 1978 ».

IV. ENFANCE MALTRAITEE

La lutte contre l'enfance maltraitée constitue l'une des priorités des politiques sociales de notre pays. Et à problème prioritaire, moyens exceptionnels...

La loi du 10 juillet 1989 relative à la prévention des mauvais traitements à l'égard des mineurs a institué un dispositif jusqu'alors inédit : le Service national d'accueil téléphonique pour l'enfance maltraitée (SNATEM), chargé de la mise en œuvre d'un numéro vert, le 119, baptisé « allô enfance maltraitée ».

Dispositif de signalement téléphonique des cas de maltraitance, le 119 est rapidement apparu comme un mode de prise en charge particulièrement adapté pour compléter les dispositifs locaux d'intervention social ou judiciaire déjà existants. En effet, la disponibilité de ce service, ouvert 24 heures sur 24, la possibilité pour l'appelant d'être assuré d'une réponse immédiate — tout en gardant l'anonymat s'il le souhaite — et de bénéficier d'un soutien psychologique, l'efficacité des actions entreprises au plan local, ont constitué autant de facteurs qui expliquent que le SNATEM ait été amené à traiter, depuis sa mise en place en 1990, un nombre sans cesse croissant d'appels téléphoniques (deux millions en 1999).

Cette réussite a d'ailleurs conduit le législateur à retenir une solution comparable dans le cadre de la lutte contre les discriminations raciales avec la mise en place du numéro vert 114 que la CNIL a eu l'occasion d'examiner en cette année 2000 (cf. infra).

Pour faire face à l'afflux des appels reçus au 119 et répondre au mieux à ses missions légales, le SNATEM s'est progressivement tourné vers une gestion informatisée.

Le traitement d'un appel adressé à « allô enfance maltraitée » est aujourd'hui le suivant :

— Toute personne composant le 119 est dirigée vers un premier service d'accueil chargé d'orienter les appels exploitables vers une plate-forme d'écoutants spéciali sés composée notamment de psychologues, de travailleurs sociaux, de juristes et de médecins.
— Chaque appel parvenant aux écoutants professionnels du SNATEM donne lieu à l'ouverture d'une « fiche d'entretien » informatisée comportant le nom de l'écoutant, l'heure, la nature de l'appel et les suites apportées.
— La majorité des appels aboutit à une aide immédiate du Service (information sur son fonctionnement, sur les démarches à effectuer pour signaler un enfant en danger, sur les organismes compétents proches de l'appelant).
— Pour les appels dénonçant des faits de maltraitance, une procédure particulière est mise en œuvre : ces appels font en effet l'objet d'un « compte rendu d'appel télé phonique », également informatisé, comportant notamment des données relatives à l'appelant, à la victime et à son contexte familial, au maltraitant présumé et à la na ture des mauvais traitements. Plus de six mille cas de maltraitance ont ainsi été enre gistrés en 1999.
— Une fois validés, ces comptes rendus sont transmis sans délai aux correspondants du SNATEM au sein des services sociaux départementaux. L'objectif est en effet d'ap porter une aide rapide non seulement à l'enfant victime, mais également à la famille.

En cas d'urgence, les informations recueillies peuvent être communiquées directement au procureur de la République, voire aux services de secours compétents (police, gendarmerie, SAMU).

L'application informatique utilisée, dénommée « AGATE », permet la collecte d'informations sur des personnes concernées par des faits de maltraitance à des degrés divers : écoutant, appelant (s'il ne souhaite pas demeurer anonyme), victime présumée, auteur présumé, correspondant départemental du SNATEM.

Dès l'origine, les responsables du 119 ont choisi, dans le souci de protéger l'anonymat des personnes concernées, de ne pas faire apparaître le numéro de télé phone de l'appelant grâce à un système de brouillage au niveau de l'autocommutateur.

En revanche, le système « AGATE » permet la saisie de l'identité et de la qualité de l'auteur présumé d'actes de maltraitance, données susceptibles d'être transmises aux correspondants du SNATEM.

Lors d'un premier examen de ce dispositif en 1989 et 1990, la Commission a admis la collecte et la conservation *au* plan national de ces informations nominatives (cf délibérations n° 89-146 du 19 décembre 1989 et n° 90-068 du 12 juin 1990 portant avis sur le projet de convention constitutive du SNATEM). En effet, la conser vation de données nominatives permet aux écoutants du SNATEM d'apporter une réponse plus adaptée aux cas qui leur sont soumis, et en particulier de faire le lien entre des appels intervenus à des moments différents ou provenant de sources diffé rentes. Le SNATEM faisait valoir que près de 50 % des situations classées initiale ment sans suite donnaient lieu l'année suivante à une seconde information (par d'autres sources que le SNATEM) concernant le même enfant en danger. La détection

de ces cas grâce à une centralisation nominative devrait contribuer, à terme, à améliorer la détection des cas de maltraitance au niveau des services départementaux.

Enfin, la conservation nominative des données devrait faciliter la tâche de la Justice agissant sur plainte d'une victime plusieurs années après la commission des mauvais traitements.

L'application informatique permet également l'édition de statistiques d'activité servant de base aux études épidémiologiques du SNATEM.

Si les objectifs poursuivis par l'informatisation du 119 sont incontestablement légitimes, il est apparu nécessaire, compte tenu de la sensibilité des informations conservées dans le fichier du SNATEM, de définir des garde-fous afin d'en garantir la confidentialité et d'assurer le respect de l'intérêt et des droits des personnes identifiées dans la base de données qu'il s'agisse de l'enfant victime, de sa famille ou des personnes mises en cause.

Dans son avis favorable, rendu le 30 novembre 2000, la Commission a émis plusieurs recommandations concernant la mise à jour, la sécurisation et la conservation des données, l'information des personnes sur l'informatisation du dispositif, ou encore l'exercice de leur droit d'accès.

En premier lieu, la Commission a souligné la nécessité d'une mise à jour des données enregistrées dans AGATE. En effet, bien que le SNATEM se soit engagé à détruire les informations relatives à des cas de maltraitance non avérés dès confirmation de leur inexactitude, force est de constater que cette garantie est parfois rendue sans effet faute de transmission systématique, par les services sociaux départementaux ou les services judiciaires, des suites données aux comptes rendus d'appel. Cette situation étant susceptible de porter gravement préjudice aux personnes mises en cause à tort, la CNIL a demandé que des propositions tendant à améliorer ces procédures de transmission lui soient adressées.

Par ailleurs, la Commission a pris acte de la mise en œuvre de mesures de sécurité strictes, notamment en ce qui concerne l'accès à l'application, et le respect d'une conservation limitée des informations enregistrées à partir de supports sécurisés.

S'agissant de l'information des personnes identifiées dans AGATE, la diffusion d'une lettre personnalisée auprès de la famille faisant l'objet d'une enquête administrative avait été initialement envisagée. Cette solution a été abandonnée, le SNATEM estimant qu'il était de l'intérêt direct de l'enfant de ne pas prévoir une information systématique de ses représentants légaux. Ainsi, l'information de ces personnes se fait par l'intermédiaire du Conseil général destinataire du compte rendu d'appel téléphonique, au moment de l'évaluation de la situation.

L'article L. 226-5 du code de l'action sociale et des familles prévoit d'ailleurs, à la charge du Président du Conseil général, une information écrite des représentants légaux de l'enfant en cas de signalement judiciaire émanant de ses services.

Enfin, la CNIL a veillé à ce qu'une personne mise en cause ne puisse, dans le cadre de son droit d'accès, obtenir communication de l'identité de la personne

l'ayant accusée d'avoir commis des mauvais traitements. Il s'agit là non pas d'empêcher les victimes de dénonciation calomnieuse de réclamer sanction et réparation à l'encontre de l'appelant malveillant, pour lesquels l'accès à cette information peut être réalisée sous le contrôle de l'autorité judiciaire après dépôt de plainte, mais de protéger d'éventuelles représailles les appelants de bonne foi et notamment l'enfant.

La même préoccupation a conduit la Commission à recommander que toute communication d'informations enregistrées dans AGATE aux représentants légaux d'un enfant ne puisse intervenir qu'après un délai permettant au SNATEM de prendre l'attache du service social concerné afin de s'assurer que cette communication ne nuira pas à cet enfant.

L'ensemble de ces garanties témoigne du souci de la CNIL de voir ce dispositif de signalement téléphonique fonctionner dans des conditions permettant de préserver en toutes circonstances les intérêts vitaux de l'enfant, tout en prévenant tout risque de délation.

Délibération n° 00-063 du 30 novembre 2000 portant avis sur le projet de délibération du conseil d'administration du Service national d'accueil téléphonique pour l'enfance maltraitée (SNATEM) concernant la mise en œuvre du traitement « AGATE » de gestion des appels reçus

La Commission nationale de l'informatique et des libertés,

Saisie pour avis d'un projet de délibération du conseil d'administration du Service national d'accueil téléphonique pour l'enfance maltraitée,

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 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 modifié pris pour son application,

Vu le code de la famille et de l'aide sociale,

Vu la convention constitutive du groupement d'intérêt public chargé du Service national d'accueil téléphonique pour l'enfance maltraitée,

Après avoir entendu Monsieur Pierre Schapira en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Sur les finalités du traitement

La Commission nationale de l'informatique et des libertés est saisie par le Service national d'accueil téléphonique pour l'enfance maltraitée (SNATEM) d'une demande d'avis concernant la mise en œuvre d'un traite-

ment automatisé d'informations nominatives permettant la gestion des appels reçus dans le cadre du numéro vert 119 et faisant l'objet d'une fiche d'entretien ou d'un compte rendu d'appel téléphonique.

La Commission estime que l'article premier de l'acte réglementaire portant création du traitement doit expressément mentionner cette finalité.

Le traitement AGATE doit permettre l'orientation des appelants vers les structures d'aides les plus proches, la création de fiches d'entretien pour toute communication traitée par les écoutants de la plate-forme téléphonique, l'édition de comptes rendus d'appel téléphonique (ou notices n° 1) pour les cas nécessitant une transmission aux autorités compétentes, et l'édition de statistiques d'activité non nominatives.

Sur la nature des informations traitées

Les informations enregistrées dans AGATE ont pour origine les appels téléphoniques reçus par le SNATEM dans le cadre de ses missions légales, ainsi que les retours d'informations (notice n° 2) émanant des services destinataires des comptes rendus d'appel téléphonique.

La Commission relève que le contenu des notices n° 1 et 2 a fait l'objet d'un examen par la Commission dans le cadre de ses délibérations 89-146 du 19 décembre 1989 et 90-068 du 12 juin 1990 et que leur contenu actuel n'appelle pas d'observation complémentaire.

Sur la durée de conservation des informations

La durée de conservation des informations nominatives enregistrées dans AGATE est fixée à deux ans après la dernière collecte de données concernant un compte rendu d'appel téléphonique ou une fiche d'entretien.

Le SNATEM souhaite qu'au-delà de cette durée les informations soient archivées sur CD-ROM pendant trois années supplémentaires notamment pour pouvoir répondre aux demandes d'information des autorités judiciaires qui peuvent intervenir plusieurs années après la commission des faits eu égard aux délais de prescription des crimes et délits visés aux articles 7 et 8 du code de procédure pénale.

La Commission considère que cette demande est légitime. Elle estime toutefois que le SNATEM doit prendre l'attache de la direction des Archives de France afin que ces modalités d'archivage intermédiaire, mais aussi ultérieurement d'archivage définitif (destruction ou versement des documents aux Archives nationales), soient déterminées en accord avec cette administration.

La Commission considère que l'acte réglementaire créant le traitement doit préciser la durée de conservation des données nominatives sur support informatique.

Sur les destinataires des données enregistrées

La Commission observe que seuls les personnels habilités du SNATEM ont accès aux informations nominatives enregistrées dans AGATE.

Par ailleurs, les destinataires des comptes rendus d'appel téléphonique (notice n° 1) sont les présidents des conseils généraux et les services sociaux départementaux compétents.

Lorsque l'urgence l'impose, peuvent également être rendus destinataires de ces documents le procureur de la République, les services de police ou de gendarmerie, ainsi que les services d'aide médicale d'urgence compétents.

Sur les mesures de sécurité envisagées

Des mesures de sécurité particulières ont été prises en ce qui concerne l'accès aux locaux et à l'application AGATE par les personnels habilités, les échanges d'informations par télécopie avec les correspondants du SNATEM et les procédures de conservation des données personnelles issues d'AGATE (notices 1 et 2 conservées sur support papier). La Commission estime satisfaisantes ces dispositions.

Sur les modalités de mise à jour des informations

Le SNATEM s'est engagé à effacer les informations relatives à des cas de maltraitance non avérés dès confirmation de leur inexactitude, c'est-à-dire après avoir été rendu destinataire d'une décision administrative ou judiciaire.

L'obligation pour les départements de communiquer au SNATEM les mesures prises dans le mois suivant la transmission des notices n° 1 ne permet qu'une mise à jour partielle des données nominatives détenues par le SNATEM s'agissant en particulier des suites qui sont données aux signalements judiciaires par les conseils généraux et dont ceux-ci n'ont pas systématiquement communication.

La Commission recommande à cet égard que toutes dispositions soient prises par les parties à la convention constitutive du SNATEM pour assurer une mise à jour plus complète des informations. Elle estime nécessaire de disposer dans un délai de six mois des mesures envisagées à cet effet.

Sur l'information des personnes concernées par le traitement

En application de l'article 70 du code de la famille et de l'aide sociale, il appartient aux présidents de conseils généraux d'informer les représentants légaux de l'enfant en cas de saisine de l'autorité judiciaire. Par ailleurs, les comptes rendus d'appel téléphonique transmis par le SNATEM aux départements et susceptibles d'être communiqués aux parents par les services sociaux comportent les mentions prescrites par l'article 27 de la loi du 6 janvier 1978.

Dans la mesure où le SNATEM dispose de supports d'information (affiches, dépliants, site www.allo119.gouv.fr), la Commission recommande qu'une information générale sur les traitements de données personnelles mis en œuvre dans le cadre du 119 soit diffusée par ces moyens et qu'il soit notamment rappelé que tout signalement résultant d'imputations fantaisistes ou infondées sera susceptible d'engager la responsabilité des appelants.

Sur l'exercice du droit d'accès et de rectification

La Commission observe que toute personne identifiée dans le traitement AGATE ne peut obtenir communication que des seules données la concernant, à l'exclusion de toute information concernant des tiers, grâce à la mise en place de masques de consultation partielle permettant de ne révéler que des informations relatives au titulaire du droit d'accès.

En particulier, ces mesures doivent empêcher la communication à une personne mise en cause, dans le cadre de l'exercice de son droit d'accès, de l'identité de la personne l'ayant accusé d'avoir commis des mauvais traitements sur mineur, y compris lorsque cette personne est sous la responsabilité légale du titulaire du droit d'accès.

La Commission prend acte de cet engagement et estime nécessaire de disposer, dans un délai de six mois, des solutions techniques élaborées par le SNATEM.

La Commission considère également que l'accès par les représentants légaux d'un enfant aux informations le concernant doit s'entourer de garanties appropriées.

La Commission recommande à cet effet de prévoir un délai de réponse de nature à permettre au SNATEM de prendre l'attache du service social départemental en charge du dossier afin de s'assurer que cette communication n'est pas de nature à porter atteinte aux intérêts de l'enfant.

Compte tenu de ces observations, la commission :

Emet un avis favorable au projet d'acte réglementaire présenté par la directrice générale du SNATEM **sous réserve** que :
— l'article premier précise que le traitement a pour finalité la gestion des appels reçus dans le cadre du numéro vert 119 et faisant l'objet d'une fiche d'entretien ou d'un compte rendu d'appel téléphonique
— la durée de conservation des informations nominatives soit précisée à l'article 2 ;

Demande à être destinataire, dans un délai de six mois à compter de l'avis favorable, des modalités complémentaires retenues pour améliorer l'information des personnes identifiées dans l'application AGATE et l'exercice de leur droit d'accès, ainsi que pour renforcer les procédures de mise à jour et, le cas échéant, de suppression des données enregistrées.

V. DISCRIMINATIONS RACIALES

Le 114 est un numéro d'appel gratuit mis en place par le gouvernement en mai 2000. Il permet à toute personne qui s'estime victime ou témoin d'une discrimination raciale (diffamation, injure, provocation à la haine raciale, discriminations), de signaler les faits aux pouvoirs publics afin d'être conseillée et orientée vers les services ou associations localement compétents, puis vers les relais locaux que constituent les commissions départementales d'accès à la citoyenneté (CODAC).

Ce dispositif repose sur un constat et une conviction. Le constat : que le nombre d'actes discriminatoires ou xénophobes est bien plus important que le nombre de faits effectivement signalés à la Justice ou à la police. La conviction : que cette distorsion est de nature à faire naître le sentiment délétère que les autorités publiques ne mettent pas tout en oeuvre pour lutter contre le racisme et la xénophobie. Une telle situation ne peut que renforcer un sentiment d'exclusion et nuire au lien social ou être propice à des réflexes de repli communautaire.

Il s'agit donc pour les pouvoirs publics de mettre à la disposition de toute personne un interlocuteur de confiance, distinct, dans un premier temps au moins, des services de police ou de gendarmerie ou de l'autorité judiciaire, en offrant une nouvelle forme d'écoute et de vigilance.

Le bilan est impressionnant : depuis sa création, le 114 a reçu plus d' 1,5 million d'appels dont plus de 7 500 ayant donné lieu à transmission aux CODAC.

Le dispositif comprend trois étapes :

— la réception des signalements par un centre d'appel téléphonique national et l'élaboration de fiches de signalement,

— la transmission des cas signalés à la CODAC (Commission départementale d'ac cès à la citoyenneté) compétente au niveau départemental ;

— le suivi, au niveau national, du traitement des cas signalés et de la suite qui leur a été donnée afin de disposer d'un instrument d'évaluation et de mesure de l'efficacité du dispositif.

Les appels reçus au 114 sont orientés vers des « écoutants » spécialement formés qui prennent note, à partir de fiches préétablies, de la nature de l'appel afin que le cas signalé puisse être traité. Les fiches d'appel ne comportent jamais la mise en cause d'une personne physique nommément désignée en tant qu'auteur de discrimination raciale. Seuls des institutions ou organismes peuvent être désignés (entreprise, établissement public, administration, etc.).

Aucun système d'identification du numéro de téléphone de l'appelant n'est mis en œuvre, ce dernier pouvant souhaiter demeurer anonyme. Dans cette hypothèse, l'écoutant invite son interlocuteur à s'adresser au secrétariat de la CODAC du département concerné ou, selon le cas, aux services publics, organisations syndicales ou associations locales de ce département. Une fiche d'appel est dressée qui ne comporte, par hypothèse, que l'identification de l'organisme accusé de discrimination. Il convient en outre de relever que l'identité de la victime n'est jamais relevée lorsque la personne appelante est un tiers.

Des doubles des fiches nominatives établies par les écoutants du 114 sont systématiquement transmis à la CODAC du département concerné à laquelle est confié le soin d'instruire l'affaire. Le dossier est alors transmis à l'un des membres de la CODAC qui devient ainsi le « référent » de la victime. Ce référent peut donc être, selon les cas, et la disponibilité de chacun, un magistrat, un fonctionnaire, un élu local ou le représentant d'une association. Il appartient alors à ce « référent » de contacter la victime et de la rencontrer, et de mettre en œuvre les actions appropriées qui, selon les cas, peuvent consister à informer la victime sur ses droits, à entreprendre une médiation, à saisir l'administration concernée en demandant qu'une enquête administrative soit menée sur les faits ou à saisir l'autorité judiciaire.

Dans la mesure cependant où, d'une part, le système aboutit à la rédaction de fiches sur les faits dénoncés qui peuvent identifier, à la fois l'appelant, qui pourra être la victime du fait discriminatoire ou un proche de la victime, et la personne morale mise en cause et où, d'autre part, ces fiches pourront être conservées dans des fichiers, voire traitées informatiquement, tant au niveau national du centre d'appel, que dans chaque département (au niveau des CODAC), le ministère

de l'Emploi et de la Solidarité a souhaité recueillir l'avis de la CNIL sur les précautions à prendre au regard des dispositions de la loi du 6 janvier 1978.

La CNIL, pleinement consciente de l'intérêt du dispositif, a souhaité appeler l'attention des pouvoirs publics sur la nécessité d'en assurer la sécurité juridique et sur les précautions à prendre pour garantir que l'objectif que le gouvernement lui assigne puisse être atteint dans le respect des droits des personnes concernées. Ainsi, la CNIL a, dans sa délibération du 8 juin 2000, rappelé que « le principe de mise à disposition d'un numéro d'appel gratuit et les garanties dont son fonctionnement doit être entouré devraient être établis par la loi, comme cela avait été le cas pour le numéro d'appel concernant l'enfance maltraitée (SNATEM) ».

Cette demande a été entendue. Lors de l'examen devant l'Assemblée nationale, en première lecture, le 12 octobre 2000, d'une proposition de loi relative à la lutte contre les discriminations, la ministre de l'Emploi et de la Solidarité a déposé un amendement visant à consacrer l'existence du 114. La ministre, lors de la discussion de l'amendement, a indiqué que le fondement législatif s'avérait tout particulièrement nécessaire dès lors que les signalements opérés peuvent donner lieu à des suites judiciaires qui sont elles-mêmes étroitement encadrées par la loi. Cet amendement a été adopté à l'unanimité par l'Assemblée nationale et constitue le nouvel article 8 de la proposition de loi. Cet article, modifié en première lecture au Sénat, a été adopté dans des termes identiques en deuxième lecture à l'Assemblée.

La CNIL a, par ailleurs, formulé plusieurs suggestions sur le fond.

Compte tenu de la sensibilité des informations traitées, la Commission a demandé que des mesures de sécurité particulières soient prises tant au niveau du centre d'appels que des CODAC afin de garantir la confidentialité des informations traitées. Elle a, à cet égard, considéré que la centralisation, au niveau national et sous une forme directement nominative, de l'ensemble des fiches d'appel et de suivi n'était pas justifiée et que le suivi des cas signalés pouvait être réalisé par la transmission, par les CODAC au niveau national, de fiches de suivi ne comportant que des numéros d'ordre, seule la CODAC disposant de l'identité de la victime et du numéro d'ordre correspondant.

La CNIL a également considéré que les informations nominatives concernant une affaire ne devraient être conservées par la CODAC que jusqu'à sa mission accomplie, ou, le cas échéant, la médiation achevée, la procédure judiciaire clôturée ou l'enquête administrative rendue.

La Commission a enfin demandé que les personnes soient clairement informées du fonctionnement du dispositif et des droits qui leur sont reconnus par la loi du 6 janvier 1978. Enfance maltraitée ou discrimination raciale : les objectif sont également légitimes, les précautions destinées à éviter toute dérive doivent être de même nature.

Délibération n° 00-033 du 8 juin 2000 relative à une demande de conseil présentée par le ministère de l'Emploi et de la Solidarité sur la mise en oeuvre du numéro d'appel gratuit — le 114 — destiné à lutter contre les discriminations raciales

La Commission nationale de l'informatique et des libertés, Saisie par le directeur de la population et des migrations du ministère de l'Emploi et de la Solidarité d'une demande de conseil relative à la mise en place d'un numéro d'appel gratuit — le 114 — destiné à lutter contre les discriminations raciales

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, notamment son article 5 ;

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

Vu la circulaire du Premier ministre du 2 mai 2000 ;

Vu la circulaire du 10 mai 2000 du ministre de l'Intérieur et du ministre de l'Emploi et de la Solidarité ;

Formule les observations suivantes :

La mise en place de ce numéro d'appel a fait l'objet d'une circulaire du Premier ministre aux préfets, datée du 2 mai 2000, et d'une circulaire sous le double timbre du ministre de l'Emploi et de la Solidarité et du ministre de l'Intérieur datée du 10 mai 2000.

Il résulte de ces textes que ce numéro d'appel gratuit est destiné à permettre aux personnes s'estimant victimes de discriminations raciales de disposer d'un conseil, notamment pour être orientées vers les services ou les associations localement compétents. Aucun système d'identification du numéro de téléphone appelant n'est mis en place, les personnes appelant ce numéro pouvant, au demeurant, conserver l'anonymat. Des fiches seront établies pour chaque appel mentionnant notamment les caractéristiques de la discrimination signalée. En aucun cas, ces fiches ne pourront comporter l'identification de l'auteur supposé de la discrimination s'il s'agit d'une personne physique, la seule indication alors portée sur la fiche consistant à préciser s'il s'agit d'un voisin, d'un collègue de travail, d'un agent d'un service public ou d'une personne ne relevant d'aucune de ces trois catégories. En revanche, les fiches d'appel comporteront la désignation des personnes morales (publiques ou privées) mises en cause, ou des entités qui en dépendent.

Ces fiches d'appel seront transmises aux secrétariats permanents des commissions départementales d'accès à la citoyenneté (CODAC) qui, créées par une circulaire du ministre de l'Intérieur du 18 janvier 1999, sont présidées par le préfet et composées notamment de représentants de l'autorité judiciaire, des services déconcentrés de l'Etat, des services publics, d'élus locaux, d'associations et des organisations représentatives des salariés et des employeurs. Dès réception de la fiche d'appel et sauf dans le cas où la fiche aura été établie à partir d'un appel anonyme, la CODAC désignera nommé-

ment un de ses membres pour rencontrer la personne qui s'estime victime d'une discrimination et accomplir les diligences appropriées. Il résulte de la fiche de suivi qui a été transmise à la CNIL que le « réfèrent » désigné par la CODAC pourra, selon le cas, informer la victime sur ses droits, entreprendre une médiation, saisir l'administration mise en cause afin qu'une enquête administrative puisse être, le cas échéant, diligentée ou saisir l'autorité judiciaire.

Tous les mois, une fiche de suivi du signalement devra être adressée au ministère de l'Emploi et de la Solidarité et au ministère de l'Intérieur sous l'autorité duquel les CODAC sont placées. Le préfet est en outre chargé d'établir un rapport semestriel des cas signalés et traités dans le département, rapport qui doit être adressé aux ministères concernés, au comité de pilotage du 114 et au groupement d'intérêt public dénommé « groupe d'études sur les discriminations (GIP-GED) », à charge pour ce dernier d'établir un rapport annuel sur la discrimination raciale en France.

L'ensemble de ce dispositif est présenté par les pouvoirs publics comme étant de nature à lutter contre les discriminations raciales, à mieux apprécier le sentiment de xénophobie ou de racisme, et à éviter toute situation dans laquelle une personne s'estimant victime d'une telle discrimination raciale nourrirait le sentiment qu'elle n'a pas l'écoute de la République.

La Commission, pleinement consciente de l'intérêt du dispositif, croit devoir appeler l'attention des pouvoirs publics sur la nécessité d'en assurer la sécurité juridique et sur les précautions à prendre pour garantir que l'objectif que le Gouvernement lui assigne puisse être atteint dans le respect des droits et libertés des personnes concernées.

A ces différents titres, le principe de mise à disposition de ce numéro d'appel gratuit et les garanties dont son fonctionnement doit être entouré devraient être établies par la loi, comme cela avait été le cas pour le numéro d'appel concernant l'enfance maltraitée.

Les dispositions législatives et réglementaires devraient notamment prendre en compte les observations suivantes :

1) La centralisation au niveau national, qu'elle soit opérée par l'organisme gestionnaire du centre d'appel ou par les deux ministères concernés, de l'ensemble des fiches d'appel et de suivi qui comportent notamment l'identification des personnes physiques ayant signalé un fait discriminatoire n'est pas justifiée par l'objectif poursuivi. Aussi, la Commission estime-t-elle que le suivi, au niveau national, des appels et des actions entreprises par les CODAC ne devrait s'opérer qu'à partir de fiches préalablement anonymisées qui comporteraient uniquement le numéro d'ordre de la fiche adressée aux CODAC, sans que l'identité de l'appelant soit conservée. De la même façon, les fiches de suivi susceptibles d'être transmises au ministère de l'Intérieur, d'une part, au ministère de l'Emploi et de la Solidarité, d'autre part, devraient être préalablement anonymisées.

2) La Commission rappelle qu'en application des principes généraux de la protection des données personnelles et notamment de l'article 5-e) de la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe, les données à caractère personnel faisant l'objet d'un traitement automatisé ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Aussi, dans la mesure où les informations

détenues par les CODAC seraient enregistrées dans un traitement automatisé, les informations qui revêtent un caractère directement nominatif (tel est le cas des informations relatives aux appelants) ou indirectement nominatif (tel pourrait être le cas d'un certain nombre d'organismes mis en cause lorsque leur seule désignation permettrait d'identifier de manière univoque une personne physique), ne sauraient-elles être conservées une fois la mission des CODAC accomplie, ou, le cas échéant, la médiation achevée, la procédure judiciaire clôturée ou l'enquête administrative rendue.

3) Des mesures particulières de sécurité devraient être prises, tant par la plate-forme d'appel que par les secrétariats permanents des CODAC, afin de garantir la confidentialité des informations collectées.

4) La plaquette d'information du public sur le 114 devrait être complétée afin de préciser, d'une part, que le dispositif n'est pas un dispositif judiciaire et, d'autre part, que tout détournement de son objectif qui résulterait d'impu tations fantaisistes ou infondées serait susceptible d'engager la responsabili té des appelants.

5) Dès lors que les fiches seraient organisées sous forme de fichiers manuels ou de traitements automatisés, l'ensemble des personnes physiques concer nées devraient être clairement informées de l'existence du droit d'accès et de rectification qui pourrait trouver à s'exercer auprès du secrétariat de la CODAC.

6) Les informations nominatives recueillies auprès des personnes appelant le 114 étant susceptibles, directement ou indirectement, de relever des catégo ries particulières d'informations énumérées à l'article 31 de la loi du 6 jan vier 1978, leur conservation dans un fichier manuel ou un traitement automatisé est subordonné au recueil de l'accord exprès des personnes concernées, sauf autorisation par décret en Conseil d'Etat pris après avis de la CNIL.

7) L'avenant à la convention constitutive du groupement d'intérêt public dé nommé « groupe d'études sur les discriminations » devrait prévoir la durée de conservation des informations traitées, les mesures de sécurité prises pour assurer la confidentialité des informations recueillies, ainsi que les des tinataires des informations traitées.

Chapitre 3

LE STIC SUITE...

Le STIC a connu de nombreuses vicissitudes.

Un premier dossier concernant cette application a été déposé à la CNIL en juin 1994 par le ministère de l'Intérieur. Compte tenu de l'ampleur du projet ministériel, l'instruction du dossier a nécessité plusieurs réunions de travail et des visites sur place. Ce dossier a été retiré à plusieurs reprises par le ministère de l'Intérieur, ce qui a conduit la Commission, après un débat en séance plénière, à appeler l'attention du Premier ministre sur ce fichier par un courrier du 11 décembre 1997. Dans sa réponse du 23 février 1998, le Premier ministre a fait connaître à la Commission qu'il avait demandé au ministère de l'Intérieur, « en liaison avec le garde des sceaux, ministre de la Justice et le ministre de la Défense », de préparer un nouveau dossier de demande d'avis.

C'est ce nouveau dossier que la Commission a examiné et qui a fait l'objet d'une délibération du 24 novembre 1998 [12]. Cette délibération qui portait avis favorable était assortie de nombreuses réserves.

La délibération de la CNIL, la polémique qui s'en est suivie puis l'avis postérieurement rendu par le Conseil d'Etat ont déterminé le ministère de l'Intérieur à revoir le dossier sur plusieurs points.

L'instruction de la nouvelle demande d'avis

C'est dans ces conditions que la Commission a été saisie d'une nouvelle demande d'avis en janvier 2000. L'instruction du dossier a nécessité des demandes de compléments et deux visites sur place au ministère de l'Intérieur.

[12] Cf 19e rapport d'activité pour 1999.

A la lumière des réactions et débats suscités par le STIC en 1998, la Commission a estimé utile de procéder à l'audition des organisations représentatives des professionnels concernés par le STIC : policiers, magistrats, avocats. La Ligue des droits de l'homme et le collectif « informatique, fichiers et citoyenneté » qui regroupe de nombreuses associations sensibilisées aux problèmes « informatique et libertés », ont été également entendus. Au total, treize organisations ont été auditionnées les 13 et 14 juin 2000.

II. LES CARACTERISTIQUES DU STIC

1 — Le système de traitement des infractions constatées (STIC) a pour objet d'enregistrer dans un fichier informatique unique les informations recueillies par les fonctionnaires de la police nationale dans le cadre de leurs missions de police judiciaire, concernant les crimes, les délits et six catégories de contraventions de 5e classe[13].

2 — Le STIC est alimenté à partir des comptes rendus d'enquête qui se présentent sous la forme normalisée d'un procès-verbal de synthèse qui est joint au dossier de procédure lorsque celui-ci, considéré comme complet par l'officier de police judiciaire qui la diligente, est transmis, selon le cas, au Parquet ou à la juridiction d'instruction. Le ministère de l'Intérieur n'exclut pas qu'à terme, le STIC puisse être alimenté directement et automatiquement, lors de la saisie du compte rendu d'enquête. Mais tel n'est pas encore le cas, puisque à l'heure actuelle la « montée en charge » du STIC s'effectue à partir du fichier des faits constatés et élucidés (FCE), déjà déclaré auprès de la Commission.

3 — Comme pour tout fichier de police, les informations seront donc saisies lors de la phase policière de l'enquête[14], par un fonctionnaire du ministère de l'Intérieur, et sans que ces informations aient été « validées » par un magistrat ou par une juridiction pénale. Il s'agit là, compte tenu des autres caractéristiques du STIC, d'un point de cristallisation du débat, même si, par hypothèse, aucun fichier de police ne pourrait exister si son alimentation était subordonnée à l'intervention d'une décision

[13] Sont visées, au titre des contraventions de 5e classe, les infractions suivantes : les violences volontaires avec incapacité totale de travail inférieure ou égale à huit jours, le racolage, la destruction ou la dégradation volontaire d'un bien appartenant à autrui avec dommage léger, le port ou l'exhibition d'uniformes, d'insignes ou d'emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité, l'intrusion dans les établissements scolaires, la provocation non publique à la discrimination, à la haine ou à la violence raciale.

[14] Trois types d'enquête peuvent être menés par les services de police :

1 - L'enquête est dite de flagrance lorsque l'infraction vient de se commettre. Dans ce cas, elle est ouverte d'office par les officiers de police judiciaire qui doivent en informer aussitôt le procureur de la République. La police judiciaire dispose de pouvoirs étendus d'investigation (perquisitions et saisies en tout lieu) pendant une durée de 10 jours et opère sous la direction du procureur de la République. Depuis la loi du 15 juin 2000, un simple témoin ne peut plus être placé en garde à vue dans ce cas.

2 - L'enquête est dite préliminaire lorsque la circonstance de flagrance n'est pas réunie (l'infraction est révélée tardivement ou portée tardivement à la connaissance de la police). L'enquête préliminaire peut être diligentée sur instruction du procureur de la République ou d'office par les personnels de police judiciaire. Les perquisitions et les saisies ne peuvent être pratiquées qu'avec le consentement exprès des personnes concernées. Un simple témoin ne peut pas être placé en garde à vue.

- L'enquête sur commission rogatoire est diligentée à la demande d'un juge d'instruction, saisi des faits et qui délègue ses pouvoirs à la police judiciaire.

judiciaire, qui est le plus souvent rendue plusieurs années après la commission de l'infraction.

4 — Le fichier poursuit plusieurs finalités dont les deux principales sont les suivantes : il s'agit d'une part pour le ministère de l'Intérieur de disposer d'un outil statistique fiable (l'annexe à la loi du 21 janvier 1995 précisait que le « système de collecte de la statistique » n'était pas satisfaisant) ; il s'agit d'autre part de permettre d'orienter les enquêtes et, le cas échéant, d'identifier les auteurs d'infractions, grâce à des recoupements avec des affaires précédentes.

Ainsi, l'interrogation du STIC peut s'effectuer, pour une recherche simple, à partir d'un ou deux critères, tels que le nom et la date de naissance d'une personne : il s'agira alors de vérifier les antécédents d'une personne déterminée. Des recherches complexes, à partir d'un nombre plus important de critères d'interrogation, permettront également de rechercher, à partir du *modus operandi* ou des éléments de signalement d'un auteur d'infraction en fuite, les affaires ou les individus approchants.

5 — L'une des finalités du fichier étant de faciliter les recherches criminelles à partir des précédents, les informations enregistrées sont appelées à être conservées pour de longues durées, et s'échelonnent de 5 à 40 ans, selon les cas.

6 — Le STIC est appelé à être consulté directement par de nombreux fonc tionnaires du ministère de l'Intérieur. Il est aujourd'hui déployé dans les circonscrip tions de sécurité publique (480 commissariats), dans les services de police judiciaire de la préfecture de police de Paris, et dans tous les services de police qui exercent une mission de police judiciaire (SRPJ, offices centraux de police judiciaire, police de l'air et des frontières, service des courses et jeux des renseignements généraux, DST, compagnies autoroutières de CRS).

En outre, les militaires de la gendarmerie sont appelés à être destinataires des informations. A l'heure actuelle, 19 militaires de la gendarmerie nationale sont habilités à consulter le STIC à partir de terminaux implantés à Rosny-sous-Bois.

Au soutien de son projet, le ministère de l'Intérieur fait valoir quatre observations principales.

En premier lieu, la nouveauté du STIC ne serait que relative, la police ayant de tout temps disposé de fichiers, plusieurs fichiers informatisés d'envergure ayant été régulièrement déclarés à la CNIL depuis 1978.

Ainsi en est-il tout particulièrement pour le fichier des faits constatés et élucidés (FCE), qui a été présenté en 1985 à la Commission comme ayant deux objets : d'une part, l'enregistrement des informations nominatives, concernant la victime et l'auteur présumé de l'infraction, issues du registre des crimes et délits tenu par chaque commissariat, d'autre part, l'établissement de tableaux statistiques de la délinquance, transmis au niveau central (cf. délibération n° 84-33 du 2 octobre 1984 et arrêté du 10 janvier 1985). Les informations sont conservées dans ce fichier pendant 400 jours, puis archivées sur support magnétique pendant 10 ans. C'est à partir de cette application informatique que les informations sont actuellement enregistrées dans le STIC.

La Commission a rendu, par ailleurs, un avis favorable aux fichiers de travail mis en œuvre par les services régionaux de police judiciaire et les brigades spécialisées (délibérations n° 91-091 et 91-092 du 8 octobre 1991). Les informations sont conservées dans ces fichiers pendant 20 ans.

La Commission a aussi donné un avis favorable au fichier automatisé des empreintes digitales (délibération n° 86-102 du 14 octobre 1986), qui constitue un fichier national alimenté par les empreintes relevées dans le cadre d'une enquête pour crime ou délit, qu'elle soit menée par les fonctionnaires de la police nationale ou par les militaires de la gendarmerie, dès lors qu'elles concernent « des personnes contre lesquelles des indices graves et concordants de nature à motiver leur inculpation auront été réunis ou des personnes, mises en cause dans une procédure pénale, dont l'identification certaine s'avère nécessaire ». Les informations, y compris celles relatives à la nature de l'affaire et à la référence de la procédure, sont conservées 25 ans à compter de l'établissement de la fiche, sans qu'il soit distingué selon la nature de l'infraction.

En deuxième lieu, le ministère de l'Intérieur fait valoir que la centralisation dans un seul et même fichier d'informations aujourd'hui éparses est de nature à faciliter le contrôle du fichier, tant en ce qui concerne les informations qui y sont enregistrées que l'usage qui en est fait. Ainsi, un système dit de « journalisation » conserve trace, pour toute interrogation du STIC, de l'identification personnelle du fonctionnaire qui l'aura consulté, du nom de la personne objet de la recherche et des date et heure précises de la consultation, et permet de s'assurer du respect de la finalité du fichier dans des conditions beaucoup plus rigoureuses qu'à l'égard de fichiers épars.

En troisième lieu, le ministère de l'Intérieur fait valoir que la rationalisation du recueil et de l'exploitation des informations de police judiciaire et leur mise à disposition des officiers de police judiciaire, quel qu'ait été le lieu de commission de l'infraction, devrait permettre de faciliter l'élucidation des crimes et délits à une époque où la délinquance est itinérante, alors que l'essentiel de la documentation criminelle demeure aujourd'hui cantonnée au niveau local.

En quatrième lieu, le ministère de l'Intérieur rappelle que le projet STIC a été présenté au Parlement dans une annexe à la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité comme devant *« fédérer au niveau national l'ensemble des fichiers de police et de documentation criminelle ».* L'annexe à la loi précisait qu'il s'agissait d'un *« système traitant toutes les informations relatives aux crimes et délits qui fournira à tout policier exerçant une activité de police judiciaire, [...] une aide à l'enquête par l'exploitation des informations relatives aux personnes et aux objets, une connaissance de la délinquance par l'exploitation de statistiques et une assistance bureautique pour la création des actes de procédure ».*

III. LES PRINCIPALES OBSERVATIONS FORMULÉES LORS DES AUDITIONS

A ce stade, trois observations principales méritent d'être rappelées comme constituant les principales réserves qui ont été formulées par les associations auditionnées sur le projet pris dans son ensemble.

La première observation porte sur les multiples finalités assignées au fichier. Outil statistique, d'une part, le fichier doit naturellement être exhaustif. Mais cette finalité ne justifie sans doute pas la conservation pendant de longues durées des informations qui y figurent. Fichier de recherche criminelle, d'autre part, le STIC doit permettre de recouper les caractéristiques d'une infraction avec des précédents *(modus operandi,* « profil » des victimes qui pourra permettre d'identifier l'auteur de certaines infractions, arme du crime qui pourra être rapprochée d'autres crimes précédemment commis — armes à feu, véhicules, etc.). Cette finalité ne peut être réalisée que si les informations sont conservées pendant de longues durées. Mais cette dernière finalité ne justifierait pas alors la conservation de l'ensemble des délits et de cinq catégories de contraventions, et devrait être réservée aux infractions les plus graves.

En mêlant l'une et l'autre de ces finalités, le STIC dérogerait aux principes généraux de protection des données et, à tout le moins, à un principe de « spécialité » des fichiers de police qui a pu être évoqué (fichier « généraliste » mais de portée locale ou bien fichier national, mais alors spécialisé : fichier terroriste, fichier des empreintes digitales, fichier des empreintes génétiques, etc.).

La deuxième observation porte sur les critères d'inscription au fichier et à l'absence de contrôle judiciaire de la réalité des faits et de la qualification de l'infraction. A cet égard, le STIC déroge sans doute moins qu'il n'est soutenu aux règles « ordinaires » des fichiers de police. Mais ce qui est redouté, et qui a été exprimé avec force notamment par le Conseil national des barreaux et la Conférence des bâtonniers, c'est qu'une imputation diffamatoire ou une accusation malveillante puisse provoquer le « fichage » d'une personne pendant 20 ans sans possibilité de voir ces informations supprimées du fichier.

Cette observation soulève la délicate question du contrôle de l'inscription et de l'efficacité ou de la portée de la mise à jour des informations.

La troisième observation porte sur l'usage qui sera fait d'un fichier aussi exhaustif. L'inquiétude exprimée par les organisations représentatives d'avocats et de magistrats (à l'exception de l'une d'entre elles) est que le STIC se transforme en un « casier judiciaire bis » qui figurerait en procédure au titre des éléments de personnalité de l'intéressé. Une telle utilisation, qui semble avérée, aux dires de plusieurs de nos interlocuteurs, marginaliserait ainsi le casier judiciaire sans offrir les mêmes garanties de certitude de la culpabilité, de durée limitée des informations, d'effacement de certaines informations passé un certain délai en cas d'amendement du condamné ou encore d'amnistie ou de réhabilitation judiciaire.

IV. LES GARANTIES APPORTEES PAR LA COMMISSION

Un plus strict encadrement de la finalité de recherche criminelle du fichier

Les craintes exprimées par de nombreux interlocuteurs lors des auditions que le STIC soit utilisé comme un « casier judiciaire bis » alors qu'il n'offre pas les garanties prévues pour le fonctionnement du casier judiciaire national, ont conduit la Commission à veiller à ce que la finalité exclusivement policière du fichier soit rigoureusement respectée.

Le respect de ce principe doit interdire que la liste récapitulative des informations ou les différentes fiches concernant une même personne, telles qu'elles résultent du STIC, puissent figurer dans le dossier de la procédure, comme les associations de magistrats et d'avocats le déplorent ou le redoutent.

Une telle prescription n'interdira évidemment pas aux policiers d'utiliser le STIC pour orienter leurs recherches dans le cadre de leurs missions de police judiciaire, ou de procéder à des rapprochements avec d'autres procédures, mais, s'agissant du passé judiciaire de l'intéressé, seul le casier judiciaire doit faire foi.

Aussi la CNIL a-t-elle souhaité que le projet de décret soit complété sur ce point et, dans le souci que toutes les conséquences soient tirées de cette prescription, demandé que seuls les magistrats du Parquet puissent être destinataires des informations figurant dans le STIC, signifiant ainsi que la liste récapitulative des infractions, telle qu'elle pourrait résulter du STIC, ne soit en aucun cas jointe à la procédure au titre des éléments de personnalité.

Il convient en outre de rappeler qu'à la suite du précédent avis émis par la Commission en 1998 sur ce traitement, en aucun cas, le STIC ne pourra être consulté dans le cadre des enquêtes administratives dites « de moralité », là encore, seul le casier judiciaire devant faire foi.

Une définition plus rigoureuse des personnes mises en cause

A la différence du précédent dossier, le projet de décret soumis à la Commission donnait une définition du « mis en cause » comme étant « *la personne contre laquelle sont réunis lors de l'enquête préliminaire, de l'enquête de flagrance ou sur commission rogatoire des indices ou des éléments attestant sa participation à la commission d'une infraction* » (article 5 du projet).

Cette définition consacrait celle qui avait été retenue par la CNIL dans sa délibération du 24 novembre 1998 pour, d'une part, préciser qu'en aucun cas un simple témoin ne saurait être fiché et, d'autre part, pour éviter qu'une personne puisse l'être sur le seul fondement de suspicions ou d'une dénonciation non étayées.

La CNIL n'avait cependant pas à l'époque demandé que cette définition figure dans l'acte réglementaire.

La définition retenue par le projet de décret a cependant été sévèrement critiquée par la plupart des personnes auditionnées, à l'exception des représentants des organisations policières, encore que l'une d'entre elles estime qu'elle devrait relever de la loi. Toutes les organisations entendues ont souhaité, en tout état de cause, que le critère d'inscription dans le fichier soit précis et simple de mise en oeuvre.

En réalité, le principal reproche fait à la définition retenue par le ministère de l'Intérieur est de ne correspondre à aucune des dispositions du code de procédure pénale.

Or, plusieurs articles du code de procédure pénale comportent des notions qui pourraient constituer des références utiles pour définir le « mis en cause ». Deux d'entre elles méritent d'être citées.

La première référence est celle de l'article *77,* alinéa premier, du codé de procédure pénale relatif à la garde à vue : *« personne à l'encontre de laquelle il existe des indices faisant présumer qu'elle a commis ou tenté de commettre une infraction ».* Cette définition a été introduite dans le code de procédure pénale par la réforme du 4 janvier 1993 pour interdire le placement en garde à vue d'un simple témoin en cas d'enquête préliminaire. Il n'est pas apparu cependant possible de retenir une telle définition dans la mesure où elle est moins rigoureuse que celle proposée par le ministère de l'Intérieur dans son projet.

La deuxième référence possible est celle de l'article 105 du code de procédure pénale, qui retient les termes « *d'indices graves et concordants d'avoir participé aux faits ».* Cet article a pour objet d'interdire qu'une personne puisse continuer à être entendue, lorsqu'une information judiciaire est ouverte et que les policiers travaillent sur commission rogatoire du juge d'instruction, sans bénéficier des droits de la défense (audition par un magistrat, assistance d'un avocat, accès au dossier dans les conditions prévues par le code de procédure pénale).

Cette définition, compte tenu de la référence faite à la gravité et à la concordance des indices, est plus rigoureuse que celle retenue dans le projet de décret. Il s'agit d'ailleurs de la définition retenue comme critère d'inscription dans le fichier automatisé des empreintes digitales géré par le ministère de l'Intérieur *(« empreintes relevées dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire, lorsqu'elles concernent des personnes contre lesquelles des indices graves et concordants de nature à motiver leur inculpation auront été réunis »* (cf. décret n° 87-249 du 8 avril 1987).

Aussi la CNIL a-t-elle demandé que cette dernière définition soit retenue par le projet de décret. Elle présente l'avantage d'être parfaitement connue des policiers et magistrats, de constituer déjà le critère de référence pour un fichier national de police, et paraît de nature à apaiser les craintes légitimes de ceux qui pouvaient

redouter que l'on puisse être fiché dans le STIC sur la foi d'une simple suspicion non étayée.

Une attention particulière aux victimes d'infractions

Le fait que les victimes d'infractions puissent être visées par le STIC avait ému l'opinion qui estimait qu'elles n'avaient pas à être « fichées » comme le sont les auteurs d'infractions.

En réalité, les auditions menées dans le cadre de la nouvelle instruction du dossier ont cependant montré que chacun s'accordait à reconnaître l'utilité de la conservation d'une telle information dans le STIC, non seulement pour pouvoir entrer en contact avec les victimes lors de l'arrestation de l'auteur de l'infraction (nécessité d'une reconnaissance de l'auteur par la victime, restitution des objets volés, information des compagnies d'assurance), mais aussi parce que, dans certains cas, et tout particulièrement dans le cas des infractions sexuelles ou des crimes en série, le « profil » de la victime (âge, catégorie socio-professionnelle, lieu de résidence, caractéristiques physiques) peut permettre d'identifier le « profil » criminel de l'auteur de l'infraction et faciliter ainsi sa découverte.

La Commission a admis cette manière de voir tout en prenant acte que la suggestion qu'elle avait faite dans sa délibération de 1998 était consacrée par le projet de décret : les victimes pourront s'opposer à ce que les informations nominatives les concernant soient conservées dans le fichier dès lors que l'auteur des faits aura été condamné définitivement.

Un renforcement du contrôle exercé par les procureurs de la République sur l'alimentation du fichier

Au-delà des catégories de personnes visées, la question s'est posée de savoir si la qualification des faits et l'identification des personnes concernées effectuées par les services de police ne devraient pas être mieux contrôlées par les procureurs, puisqu'aussi bien, « le traitement des informations nominatives s'effectue sous le contrôle du procureur de la République territorialement compétent ».

Lors des auditions, un syndicat de police a fait valoir que les informations peuvent être enregistrées dans le STIC avant la fin de la phase policière, que les rubriques d'alimentation du STIC ne sont pas toujours les mêmes que celles du compte rendu d'enquête joint au dossier de la procédure, que le contrôle hiérarchique n'est pas systématique. D'autres associations ou syndicats ont soutenu que la qualification des faits devait relever des magistrats.

Sans subordonner l'alimentation du STIC à une vérification préalable par le procureur, qui paraît tout à fait irréaliste, le souci de renforcer l'effectivité des garanties a conduit la Commission à proposer que le projet de décret soit complété afin de prévoir qu'une copie papier des informations enregistrées dans le STIC soit, en même temps que la procédure, systématiquement adressée au magistrat du Parquet, qui

pourra ainsi assurer son contrôle et, le cas échéant, en *cas* d'erreur ou d'appréciation divergente des faits, faire rectifier le plus rapidement possible les informations enregistrées dans le STIC.

Une définition plus rigoureuse des données sensibles susceptibles d'être collectées

Les catégories d'informations nominatives enregistrées dans le STIC sont les catégories classiques d'informations qui figurent généralement dans les fichiers de police.

Ces informations peuvent cependant relever des catégories d'informations sensibles visées par l'article 31 de la loi du 6 janvier 1978, soit qu'elles résultent de la procédure elle-même (injures raciales, agressions sexuelles, etc.), soit qu'elles résultent des éléments de signalement qui doivent être conservés pour retrouver des personnes en fuite.

En effet, la photographie ainsi que le signalement des personnes mises en cause pourront figurer dans le STIC, comme ils sont actuellement archivés dans les fichiers dits « Canonge », du nom du brigadier de police marseillais ayant conçu dans les années 50 le premier fichier mécanographique de signalements. Ces éléments sont évidemment indispensables à l'identification des auteurs d'infractions qui auront pu être décrits par la victime ou repérés par des témoins auxquels la police judiciaire présentera des photographies de personnes précédemment mises en cause.

En aucun cas, les photographies de victimes ne seront enregistrées sauf s'il s'agit de personnes disparues ou de corps non identifiés.

Aux termes de la loi du 6 janvier 1978, les données sensibles ne peuvent être collectées et conservées sans l'accord exprès de la personne concernée, sauf si un décret en Conseil d'Etat pris après avis conforme de la CNIL l'autorise. C'est cette procédure particulière qui justifie que le texte instituant le STIC doive préciser que l'application informatique peut traiter des données sensibles.

Les données sensibles énumérées par l'article 31 de la loi sont les suivantes : origines raciales, opinions politiques, philosophiques ou religieuses, appartenances syndicales, mœurs.

Depuis l'adoption des décrets relatifs aux fichiers des renseignements généraux du 14 octobre 1991, et à l'issue d'une vaste concertation menée par la CNIL auprès de l'ensemble des associations de défense des droits de l'homme, l'expression « signes physiques particuliers, objectifs et inaltérables » des personnes est préférée à la formule non dénuée d'ambiguïté qui figure dans le texte même de la loi du 6 janvier 1978 « d'origines raciales ».

L'autorisation d'enregistrer des données sensibles ne saurait bien entendu justifier que figure en procédure ou dans un fichier de police, la religion d'une personne suspectée de vol ou l'opinion politique d'une personne suspectée de proxénétisme.

Aussi la Commission a-t-elle demandé que la dérogation accordée au ministère de l'Intérieur soit davantage circonscrite. Ainsi, des informations relevant de l'article 31 ne pourront être collectées et traitées que si elles résultent de la nature ou des circonstances de l'infraction (la pédophilie pour une infraction pédophile, les « opinions politiques » pour les infractions terroristes).

Les éléments d'identification des personnes en cause (signes physiques particuliers, objectifs et permanents) pourront, eux, être enregistrés, mais, comme le prévoit le texte du gouvernement, seulement à la condition qu'ils soient nécessaires à la recherche et à l'identification des auteurs d'infractions.

Une mise à jour des informations plus rigoureuse

Le projet d'arrêté soumis à l'avis de la Commission en 1998 précisait que le traitement des informations nominatives enregistrées dans le STIC s'effectuerait sous le contrôle du procureur de la République territorialement compétent qui pourrait demander leur rectification ou leur effacement. Il était prévu de compléter ce dispositif par une circulaire du garde des Sceaux demandant aux procureurs généraux et aux procureurs de la République de transmettre systématiquement aux gestionnaires du système, les décisions de relaxe ou d'acquittement.

Dans sa délibération du 24 novembre 1998, la Commission avait estimé que ce dispositif devait être renforcé afin de reconnaître à toute personne ayant bénéficié d'une mesure de classement sans suite, d'une décision de non-lieu ou des dispositions légales portant amnistie ou réhabilitation, de demander, soit directement au procureur de la République, soit à la CNIL lors de l'exercice d'un droit d'accès, que le fichier soit complété par la mention de ces suites judiciaires ou légales.

A la suite de l'avis rendu par le Conseil d'Etat, le ministère de l'Intérieur a fait le choix de poser explicitement l'obligation faite aux procureurs de la République de transmettre aux gestionnaires du fichier l'ensemble des décisions concernées. Ainsi, le nouveau projet de décret soumis à la Commission disposait que « *pour l'application de l'article 37 de la loi du 6 janvier 1978, le procureur de la République transmet au gestionnaire du fichier les informations relatives aux décisions de relaxe ou d'acquittement devenues définitives. Il transmet également les décisions de non-lieu ou de classement sans suite motivées par l'insuffisance de charges à l'encontre du mis en cause.*

L'autorité judiciaire fait connaître au gestionnaire du fichier les faits couverts par une mesure d'amnistie. Le gestionnaire du fichier procède alors à leur effacement. »

Il résultait très clairement du texte proposé qu'à l'exception des mesures d'amnistie de certains faits, dans tous les autres cas, la mise à jour consisterait à compléter les informations et non à les effacer.

Les auditions menées dans le cadre de l'instruction du nouveau dossier concernant le STIC ont démontré, s'il en était besoin, que cette question était délicate.

Sur le fond, les relaxes et les acquittements, lorsqu'ils sont définitifs, sont revêtus de l'autorité de la chose jugée et ne peuvent plus donner lieu à une reprise des poursuites. Compte tenu des caractéristiques du STIC, de l'accessibilité des informations qu'il comporte à un très grand nombre de policiers, du fait que ce fichier est placé sous l'autorité des procureurs, il apparaît difficile de soutenir que les premières investigations policières devraient prévaloir sur la décision judiciaire finale. Aussi la CNIL a-t-elle demandé que les informations nominatives relatives aux personnes initialement mises en cause soient purement et simplement supprimées en cas de relaxe ou d'acquittement.

S'agissant des décisions de non-lieu, la Commission a estimé qu'il devait revenir au procureur de la République de prescrire l'effacement des informations lorsque le non-lieu est motivé en droit.

Enfin, s'agissant des mesures d'amnistie, la Commission a également estimé que toutes les infractions amnistiées de plein droit devaient être effacées du fichier.

En revanche, s'agissant des procédures classées sans suite, le dispositif proposé par le ministère de l'Intérieur consistant à compléter l'information par la mention du classement et non pas à les effacer a été accepté par la Commission.

La reconnaissance d'un droit d'initiative au bénéfice des personnes concernées pour provoquer la mise à jour ou l'effacement des informations les concernant

Aux termes du projet de décret soumis à la Commission, *« toute personne initialement mise en cause lors d'une enquête préliminaire ou de flagrance peut exiger que la qualification des faits finalement retenue par l'autorité judiciaire soit substituée à la qualification initialement enregistrée dans le fichier ».*

Cette prescription satisfaisait à une demande exprimée par la CNIL dans sa délibération de 1998. En revanche, le projet de décret n'évoquait pas la possibilité pour une personne ayant bénéficié d'un non-lieu, d'une relaxe ou d'un acquittement, de solliciter, directement auprès du procureur de la République ou par l'intermédiaire de la CNIL, la mise à jour des informations la concernant. Certes, à la suite de l'avis du Conseil d'Etat, le projet de décret prévoyait, désormais, dans de tels cas, une mise à jour d'office à l'initiative du procureur de la République.

Cependant, le dispositif de mise à jour des informations d'office n'est pas paru de nature à justifier la suppression du « filet de sécurité » que la CNIL avait appelé de ses vœux en 1998. Aussi, la Commission a-t-elle considéré que le projet de décret devait être complété afin de reconnaître explicitement à toute personne ayant bénéficié d'un non-lieu, d'une relaxe ou d'un acquittement le droit de saisir directement le procureur de la République territorialement compétent ou la CNIL pour que le fichier soit mis à jour dans les conditions prévues par le projet de décret.

Le raccourcissement de certaines durées de conservation des informations

Aux termes du projet de décret, la durée de conservation des informations enregistrées dans le STIC diffère selon les catégories de personnes concernées. Le ministère de l'Intérieur a sur ce point repris toutes les suggestions qui avaient été faites par la CNIL en 1998.

En principe, les informations concernant les « mis en cause » seront conservées 20 ans, s'ils sont majeurs, 5 ans s'ils sont mineurs. Ces règles connaissent dans les deux cas de figure des dérogations, liées à la nature de l'infraction commise.

• « mis en cause » majeurs (en principe, 20 ans) :

la durée de conservation sera réduite à 5 ans lorsque l'infraction commise est soit l'une des six catégories de contraventions enregistrées dans le STIC, soit l'un des délits prévus par le code de la route, par les articles 227-3 à 227-11 du code pénal (dispositions relatives aux abandons de famille et aux atteintes à l'exercice de l'autorité parentale), ou par l'article L. 628 du code de la santé publique (usage de stupéfiants).

en revanche, la durée de conservation sera portée à 40 ans lorsque l'infraction commise figure sur la liste établie par le ministère de l'Intérieur, jointe en annexe au décret.

les informations seront effacées lorsque les « mis en cause » atteindront 75 ans.

• « mis en cause » mineurs (en principe, 5 ans) :

La durée de conservation pourra être portée à 10 ans pour certaines infractions, énumérées sur une liste annexée, à 20 ans pour les infractions les plus graves énumérées sur une autre liste.

• pour tous les « mis en cause », qu'ils soient mineurs ou majeurs, le projet de décret prévoit que, dans l'hypothèse où une nouvelle infraction serait commise avant l'expiration de ces durées de conservation, l'ensemble des informations enregistrées serait alors conservé durant le délai le plus long.

• victimes : les informations relatives aux victimes seront conservées 15 ans au plus, les intéressés pouvant demander, dès lors que l'auteur des faits a été condamné définitivement, la suppression des informations les concernant. Toutefois, lorsque l'infraction commise porte sur des œuvres d'art, des bijoux ou des armes, cette durée de conservation sera prolongée jusqu'à la découverte des objets.

Ces durées de conservation doivent être rapprochées des durées prévues pour d'autres fichiers de police. Ainsi, le fichier des empreintes génétiques, fichier national mais qui peut comporter des informations sur de simples délits tels que l'outrage public à la pudeur, conserve les références des dossiers pendant 40 ans. Mais il convient d'avoir à l'esprit que seules des personnes définitivement condamnées y figurent. Le fichier national automatisé des empreintes digitales conserve les informations pendant 25 ans. H s'agit, comme son nom l'indique, d'un fichier national qui, comme le STIC, est alimenté lors de la phase policière de l'enquête, et peut concerner tous les crimes et délits. Il comporte le nom de la personne, ses empreintes, la nature de l'infraction et les références de la procédure. Aucune distinction n'est

établie selon la gravité de l'infraction. Le fichier des faits constatés et élucidés ne devait conserver les informations que pendant 10 ans ; les fichiers de travail des SRPJ et des brigades spécialisées conservent les informations pendant 20 ans, cette durée étant apparue justifiée au regard du type d'enquêtes qui sont confiées à ces services spécialisés dans la grande criminalité.

Au regard des durées déjà pratiquées, la Commission a observé que :
— certaines des durées fixées sont parmi les moins longues que la CNIL ait eu à connaître, qu'il s'agisse des infractions commises par les mineurs ou de certaines in fractions déterminées dont l'auteur est une personne majeure ;
— à la différence d'autres fichiers de police judiciaire, il est désormais clairement établi qu'en aucun cas, le STIC ne pourra être utilisé dans le cadre d'enquêtes de mo ralité — ce qui constitue un progrès incontestable — et qu'il sera mis à jour dans des conditions beaucoup plus rigoureuses et pouvant être beaucoup plus aisément con trôlées que d'autres fichiers ;
— les informations enregistrées dans le STIC ne pourront pas être jointes, au titre des éléments de personnalité, au dossier de procédure judiciaire.

Ainsi cantonné à sa seule finalité policière, le STIC paraît se situer dans le droit commun des fichiers policiers, sous deux réserves importantes.

Certaines infractions n'ont pas paru à la Commission nécessiter, au titre des recherches policières, une durée de conservation supérieure à 5 ans. Il en est ainsi :
— des infractions involontaires — qui ne sont pas toutes des infractions à la circula tion — telles que l'homicide involontaire et les blessures involontaires (art. 221-6 et 222-19 du code pénal),
— des infractions de détournement de gage ou d'objets saisis, incriminations qui pè sent fondamentalement sur des personnes endettées à l'égard desquelles le créancier peut décider d'agir au pénal (art. 314-5 et 314-6 du code pénal),
— du vol simple (art. 311-3 du code pénal), par opposition au vol aggravé, c'est-à-dire au vol avec effraction ou violence, ou encore commis en réunion,
— du délit d'entrave aux libertés constitutionnellement protégées (art. 431-1 du code pénal) et de participation sans arme à rassemblement interdit (art. 431-4 du code pénal).

Ces infractions sont parmi les moins réprimées par le code pénal (trois ans ou un an d'emprisonnement pour les deux dernières), et peuvent concerner un grand nombre de personnes (jeunes gens, exclus, syndicalistes, manifestants). Enfin, il s'agit d'infractions qui ne relèvent pas de la grande criminalité.

C'est la raison pour laquelle la Commission a demandé que la durée de conservation des informations se rapportant à de telles informations soit ramenée à cinq ans.

La deuxième observation portait sur la référence qui était faite à la notion de « trafics » (véhicules, or et métaux précieux, bijoux, armes), dans le document annexé au projet de décret comportant la liste des infractions devant déterminer une durée de conservation dérogatoire de 40 ans. La Commission a constaté que le trafic n'était pas une qualification pénale, sauf en matière de stupéfiants et d'infractions au régime des armes et munitions (mais ces infractions sont visées par ailleurs). Aussi

a-t-elle souhaité que cette référence disparaisse, le crime de « vol en bande organisée », en définitive, s'y substituant.

Une grande attention aux mesures de sécurité

Seuls les personnels spécialement habilités auront accès au STIC. Les habilitations personnelles sont délivrées par les chefs de service qui déterminent pour chacune des personnes qui relèvent de leur autorité son profil d'utilisateur. La politique retenue par le ministère en la matière consiste à habiliter un grand nombre de personnels de police qui occupent des fonctions d'enquêteurs, de personnels administratifs, de documentalistes (le STIC étant placé sous la responsabilité du chef du service de la documentation criminelle), ce qui évite de voir se développer une pratique consistant à se « prêter » de manière indue, entre collègues, des mots de passe d'accès au fichier.

Les procédures d'habilitation consistent à délivrer à chaque utilisateur un mot de passe personnel, renouvelé tous les trois mois, qui, associé à son matricule, lui confère des droits à consulter le STIC. Cette procédure est gérée par le logiciel CHEOPS, qui est commun à l'ensemble des traitements du ministère de l'Intérieur. En outre, un procédé de déconnexion automatique après trois tentatives infructueuses a été mis en œuvre.

Il a pu être vérifié lors des visites sur place au ministère de l'Intérieur qu'une journalisation des interrogations du STIC était mise en place. L'application CHEOPS conserve en effet une trace pendant trois ans, comme pour toute application informatique gérée par le ministère, de toutes les connexions au STIC.

Sont enregistrés le matricule du fonctionnaire du ministère de l'Intérieur, son nom, l'organisme ou le service auquel il appartient, le terminal utilisé, les date et heure de la connexion. Les critères de recherche (nom, *modus operandi,* etc.) et le nombre de réponses obtenues sont enregistrés dans un module de journalisation spécifique au STIC selon les modalités suivantes :

— pour les fonctions de consultation, les critères de recherche et le nombre de réponses obtenues,

— pour les fonctions de mise à jour (création, modification, suppression), la demande de mise à jour effectuée et toutes les opérations induites sur les fichiers constituant la base de données.

Toutes les informations tracées sont susceptibles de constituer des critères de recherche (nom de la personne, objet de l'interrogation du fichier, matricule du fonctionnaire de police, etc.). Il est ainsi possible de connaître dans le détail, sur les trois dernières années, toutes les actions (mises à jour et consultations) opérées sur un dossier ou effectuées par un fonctionnaire de police.

Le délai de réponse, qui diffère selon la nature de la demande, peut être de l'ordre de 48 heures.

Ces « historiques horodatés » des consultations sont évidemment tenus à la disposition de la Commission pour tout contrôle qu'elle souhaiterait effectuer en application de l'article 21 de la loi du 6 janvier 1978.

Enfin, toute connexion au STIC provoque l'affichage d'une page écran informant les utilisateurs que trace de la consultation qu'ils s'apprêtent à faire sera conservée à des fins de contrôle.

La Commission a appelé l'attention du ministère de l'Intérieur sur l'opportunité qu'une circulaire soit adressée à l'ensemble des fonctionnaires de police, pour leur rappeler les précautions d'emploi dont le STIC doit faire l'objet.

Un droit d'accès aménagé pour plus de transparence

Aux termes du projet de décret, le droit d'accès aux informations enregistrées dans le STIC s'exerce en application de l'article 39 de la loi du 6 janvier 1978. Cela signifie en pratique que toutes les demandes de droit d'accès doivent être adressées à la CNIL qui désigne un de ses membres, membre ou ancien membre du Conseil d'Etat, de la Cour de Cassation ou de la Cour des Comptes, pour procéder aux investigations à l'issue desquelles il est notifié, selon les termes mêmes de la loi, que « les investigations ont été effectuées ». Cette formulation laisse très souvent les requérants insatisfaits.

Aussi, suivant une recommandation précédemment exprimée par la Commission, le ministère de l'Intérieur a-t-il prévu un aménagement à ce dispositif : si la procédure est judiciairement close, après accord du procureur de la République, la Commission pourra constater, en accord avec le ministère de l'Intérieur, que des informations nominatives enregistrées ne mettent pas en cause la sûreté de l'Etat, la défense ou la sécurité publique, et qu'il y a lieu de les communiquer à la personne concernée. Il résultera de ce dispositif une plus grande transparence à l'égard de ce fichier.

Le cantonnement de l'utilisation du STIC à des fins de police administrative

Le ministère de l'Intérieur, se rangeant aux réserves exprimées par la CNIL dans son avis du 24 novembre 1998, a interdit toute consultation du STIC dans le cadre d'enquêtes de moralité ordonnées par l'autorité administrative.

Il prévoit toutefois que les personnels de la police nationale, individuellement désignés et spécialement habilités par le directeur de la police nationale ou par le préfet pourront consulter le STIC 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. Il pourra s'agir de consultations ponctuelles à l'occasion de missions particulières telles que l'organisation du déplacement d'une personnalité

étrangère ou de celle d'un événement exceptionnel (sommet de chefs d'Etat et de gouvernement, événements sportifs de grande dimension, etc).

La Commission a estimé qu'une telle utilisation du fichier n'était pas dépourvue de justification dès lors qu'étaient réunies les garanties suivantes :
seules les informations se rapportant à des affaires achevées pourront être consul tées ;
les consultations administratives ne permettront pas d'avoir accès aux informa tions se rapportant aux victimes, ni aux personnes ayant bénéficié d'une décision de non-lieu ou de classement sans suite ;
cette consultation sera réservée aux personnels de la police nationale individuel lement désignés et spécialement habilités par le directeur général de la police natio nale ou par le préfet ;
une journalisation des interrogations du fichier sera mise en place qui obéira aux mêmes règles que celles prévues pour la police judiciaire.

Une exigence de parfaite information des personnes sur leurs droits

La Commission a demandé au ministère de l'Intérieur et au ministère de la Justice de l'informer des mesures qui seront prises afin que les personnes concernées soient clairement et précisément informées de leurs droits et tout particulièrement de leur droit d'accès, de leur droit de demander rectification, mise à jour ou effacement des données les concernant.

C'est dans ces conditions et sous ces réserves que la Commission a rendu l'avis qui suit, non sans faire part au gouvernement d'une réflexion de portée plus générale.

Le code de procédure pénale est étrangement silencieux sur les fichiers de police. Il ne comporte de dispositions qu'à l'égard du casier judiciaire et, depuis la loi du 17 juin 1998, à l'égard du fichier national automatisé d'empreintes génétiques. Les seules dispositions de ce code relatives à la conservation ou à la suppression d'informations par la police concernent la photographie et les relevés d'empreintes digitales qui peuvent être pris à l'occasion d'une procédure de vérification d'identité dans l'hypothèse où une personne contrôlée refuse ou n'est pas en mesure de justifier de son identité. Dans ce cas, et si la procédure de vérification d'identité n'est suivie d'aucune enquête judiciaire, l'article 78-3 du code de procédure pénale précise que « la vérification d'identité ne peut donner lieu à une mise en mémoire sur fichiers » et que « le procès-verbal ainsi que toutes les pièces se rapportant à la vérification sont détruits dans un délai de six mois sous le contrôle du procureur de la République ».

Dans le silence législatif, c'est donc la loi du 6 janvier 1978 qui régit seule les fichiers de police et peut leur assurer un encadrement juridique. Cette situation n'est certainement pas pleinement satisfaisante au regard des intérêts publics en jeu qui paraissent considérables, qu'il s'agisse des impératifs de sécurité publique et de

sûreté des personnes, ou des garanties de libertés publiques et individuelles qui doivent leur être reconnues.

L'article premier du décret du 17 juillet 1978 autorise la Commission à proposer au gouvernement « toute *mesure législative ou réglementaire de nature à adapter la protection des libertés à l'évolution des procédés et techniques informatiques ».* Le STIC n'illustre-t-il pas cette évolution des procédés et techniques qui justifierait, à terme, une intervention législative de portée générale sur le fonctionnement et le contrôle des fichiers de police judiciaire ?

Délibération n° 00-064 du 19 décembre 2000 relative à un projet de décret en Conseil d'État portant création du « système de traitement des infractions constatées (STIC) » et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés,

Saisie par le Premier ministre d'un projet de décret en Conseil d'Etat portant création du « système de traitement des infractions constatées (STIC) » et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

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

Vu le code pénal ;

Vu le code de procédure pénale ;

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

Vu la loi d'orientation et de programmation relative à la sécurité du 21 janvier 1995 et ses annexes ;

Après avoir entendu MM. François Giquel et Gérard Gouzes, en leur rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Observe :

Le « système de traitement des infractions constatées (STIC) » est un fichier national appelé à enregistrer les informations recueillies par les fonctionnaires de la police nationale dans le cadre de leurs missions de police judiciaire relatives aux crimes, aux délits et à six catégories de contraventions de la 5^{e} classe. Les contraventions visées sont les suivantes : les violences volontaires ayant entraîné une incapacité totale ou inférieure à huit jours, le racolage, la destruction ou la dégradation volontaire d'un bien appartenant à autrui avec dommage léger, le port ou l'exhibition d'uniformes, d'insignes ou d'emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité, l'intrusion dans les établissements scolaires, la provocation non publique à la discrimination, à la haine ou à la violence raciale.

Devant être alimenté à l'issue de la phase policière de l'enquête à partir des comptes rendus d'enquêtes qui se présentent sous la forme normalisée d'un procès-verbal de synthèse, joint au dossier de la procédure, le STIC doit, selon le ministère de l'Intérieur, permettre la rationalisation du recueil et de l'exploitation des informations de police judiciaire aux fins de recherches criminelles, de production de statistiques et de gestion des archives. Il pourra aussi, dans certaines conditions, être consulté à des fins de police administrative.

Le ministère de l'Intérieur, qui fait valoir que ce projet, ancien, a été présenté au Parlement à l'occasion de l'adoption de la loi d'orientation et de programmation relative à la sécurité du 21 janvier 1995 et que ses caractéristiques principales ont été précisées dans un document annexé à cette loi et publié au Journal officiel, souligne qu'une plus grande efficacité dans la recherche des auteurs d'infractions est attendue du regroupement dans un même ensemble d'informations actuellement conservées dans des fichiers manuels ou informatiques épars, le plus souvent cantonnés au niveau local, et de leur mise à la disposition de la police judiciaire. Sans mettre en cause la légitimité des objectifs assignés à un tel fichier, la CNIL croit devoir souligner qu'une telle centralisation d'informations de police judiciaire appelle nécessairement à la vigilance et à la reconnaissance de garanties sérieuses destinées, d'une part, à prévenir tout fichage non contrôlé, erroné ou abusif des personnes, d'autre part, tout usage d'un tel fichier à des fins étrangères à celles pour lesquelles il est constitué. En l'absence de dispositions d'ordre général dans le code de procédure pénale relatives à la réglementation des fichiers de police, il appartient, en l'état, à la CNIL de veiller, conformément aux dispositions de l'article premier de la loi du 6 janvier 1978 aux termes duquel « l'informatique ne doit porter atteinte ni à l'identité humaine, ni à la vie privée, ni aux libertés individuelles ou publiques », à ce que les caractéristiques et les modalités de fonctionnement et de contrôle de cet outil nouveau pour la police judiciaire soient conformes aux principes généraux de la protection des données personnelles et aux garanties instituées par le code de procédure pénale.

1. Le contrôle de l'alimentation du fichier

La CNIL prend note que si le fichier est mis en œuvre par le ministère de l'Intérieur (direction générale de la police nationale), le projet de décret précise que le traitement des informations nominatives s'effectue sous le contrôle du procureur de la République territorialement compétent. Cette garantie est conforme aux dispositions de l'article 12 du code de procédure pénale qui précise que la police judiciaire est exercée sous la direction du procureur de la République.

1.1. Les personnes concernées

Les personnes concernées seront, d'une part, les personnes mises en cause, d'autre part, les victimes, et en aucun cas les témoins.

Seules pourront être enregistrées dans le STIC les informations relatives aux personnes dites « mises en cause » à la fin de la phase policière de l'enquête et qui figurent dans le compte rendu d'enquête, rédigé par l'officier de police judiciaire avant transmission du dossier de procédure au magistrat du Parquet ou au juge d'instruction, et joint à ce dernier.

Afin de garantir qu'en aucun cas le simple témoin d'une infraction ne puisse voir les informations le concernant enregistrées dans le fichier et qu'aucune personne ne puisse l'être sur le fondement d'un simple soupçon ou d'une dénonciation malveillante ou non étayée, il y a lieu de renforcer la rédaction proposée par le gouvernement à l'article 5 du projet de décret pour la définition du « mis en cause » en subordonnant l'inscription dans le fichier à l'existence d'indices « graves et concordants », au sens de l'article 105 du code de procédure pénale.

Le projet de décret prévoit que pourront être enregistrées les informations relatives aux victimes d'infractions. Un tel enregistrement qui pourrait paraître, en première analyse, inutilement stigmatisant pour les victimes et de nature à leur porter à un préjudice moral supplémentaire a, en réalité, pour objet de permettre aux officiers de police judiciaire d'entrer en contact avec les personnes concernées lors de l'arrestation de l'auteur de l'infraction (nécessité d'une reconnaissance de l'auteur de l'infraction par ses victimes, restitution des objets volés, information des compagnies d'assurance). En outre, l'enregistrement d'informations sur les victimes vise à permettre l'identification du « profil criminel » de l'auteur de l'infraction, notamment dans le cas d'infractions sexuelles, de crimes en série, ou d'actes de délinquance répétés.

Dans ces conditions, et pour ces motifs, la finalité du fichier paraît justifier l'enregistrement d'informations sur les victimes dès lors que ces dernières pourront demander, conformément au voeu précédemment exprimé par la Commission, que toutes les informations nominatives les concernant soient supprimées du fichier dès que l'auteur de l'infraction aura été définitivement condamné. La Commission prend acte que cette garantie est consacrée par le projet de décret dans son article 10.

1.2. Le contrôle de la qualification des faits

Les informations étant enregistrées, comme pour tout fichier de police judiciaire, à l'issue de la phase policière de l'enquête, il convient de veiller à ce que cette qualification, qui déterminera notamment la durée de conservation des informations dans le fichier, soit exacte et, le cas échéant, mise à jour.

Afin d'assurer un contrôle de la qualification des faits par les magistrats du Parquet sous le contrôle desquels le traitement des informations enregistrées dans le STIC est opéré, il y a lieu de prévoir que les informations nominatives relatives aux personnes mises en cause et aux victimes ainsi que les qualifications des faits telles qu'elles sont enregistrées dans le STIC seront systématiquement transmises au procureur de la République territorialement compétent en même temps que lui sera adressée la procédure, afin qu'il puisse user, le cas échéant, du pouvoir qui lui est reconnu par l'article 3 du projet de décret de demander la rectification ou l'effacement des informations enregistrées. Le projet de décret devra être complété sur ce point.

La CNIL prend note que le projet de décret prévoit, conformément à la demande qu'elle avait exprimée, que toute personne initialement mise en cause lors d'une enquête préliminaire ou de flagrance pourra exiger que la qualification des faits finalement retenue par l'autorité judiciaire soit substituée à la qualification initialement enregistrée dans le fichier. Cette garantie devra être étendue aux enquêtes diligentées sur commission rogatoire du juge d'instruction. Le projet de décret devra être complété en ce sens.

La CNIL estime, en outre, que le projet de décret doit prévoir la possibilité pour toute personne ayant bénéficié d'une décision définitive de relaxe ou d'acquittement, ou d'une décision de non-lieu ou de classement sans suite motivée par l'insuffisance de charges, de solliciter du procureur de la République, soit directement, soit indirectement par l'intermédiaire de la CNIL à l'occasion de l'exercice de son droit d'accès, la mise à jour des informations la concernant. Le projet de décret devra être complété en ce sens.

1.3. La mise à jour des informations

Le projet de décret fait obligation aux procureurs de la République de transmettre au gestionnaire du fichier les informations relatives aux décisions de relaxe ou d'acquittement devenues définitives ainsi que les décisions de non lieu ou de classement sans suite motivées par l'insuffisance de charges à l'encontre de la personne mise en cause, à charge pour le gestionnaire de compléter les informations par l'indication de Ta suite judiciaire donnée. De même, l'autorité judiciaire devra faire connaître au gestionnaire du fichier les faits couverts par une mesure d'amnistie, à charge pour ce dernier de procéder alors à leur effacement. Ce dispositif appelle deux réserves. S'agissant des décisions de non-lieu motivées en droit, qui sont alors revêtues de l'autorité de la chose jugée, il y a lieu de prévoir que leur notification au gestionnaire du fichier doit conduire, sur l'indication du procureur de la République, à l'effacement pur et simple des informations directement ou indirectement nominatives relatives à la personne mise en cause. Le projet de décret devra être complété en ce sens.

S'agissant des décisions définitives de relaxe et d'acquittement, qui sont revêtues de l'autorité de la chose jugée, leur notification au gestionnaire du fichier doit, de même, conduire à l'effacement des informations directement ou indirectement nominatives relatives à la personne initialement mise en cause. Le projet de décret devra être modifié en ce sens.

2. Le contrôle de l'usage du fichier

2.1. Le STIC ne doit pas être utilisé comme un casier judiciaire parallèle.

Le caractère exhaustif du STIC peut laisser craindre que ce fichier soit utilisé afin de répertorier l'ensemble des procédures pénales dans lesquelles une même personne aurait pu être mise en cause. Tel serait notamment le cas si figurait dans le dossier de procédure, au titre des éléments de personnalité des intéressés, l'ensemble des fiches répertoriées dans le STIC au nom de la personne concernée. Une telle utilisation qui marginaliserait le casier judiciaire national sans offrir les mêmes garanties de certitude de la culpabilité, d'effacement de certaines informations passé un certain délai en cas d'amendement du condamné, ou encore d'amnistie ou de réhabilitation judiciaire, serait contraire au principe de finalité du STIC qui n'a pas pour objet de répertorier des condamnations pénales, ni d'enregistrer de manière systématique les suites judiciaires des procédures établies par la police judiciaire.

Le souci de prévenir un tel risque doit conduire à compléter le projet de décret afin d'une part, de préciser que seules celles des informations enregistrées dans le STIC qui sont relatives à la procédure en cours peuvent être jointes au dossier et, d'autre part, que seuls les magistrats du Parquet sont

destinataires des informations enregistrées dans le STIC et non l'ensemble des autorités judiciaires.

2.2. Le STIC ne pourra pas être utilisé dans le cadre d'enquêtes, dites parfois de moralité, ordonnées par l'autorité administrative sur des personnes sollicitant un titre, une habilitation, une autorisation ou un agrément.

Il convient de prendre acte de ce que, en aucun cas, les informations enregistrées dans le STIC ne pourront être consultées ou utilisées dans le cadre d'enquêtes de moralité ordonnées par l'autorité administrative. En effet, en prévoyant que certaines autorités administratives sont habilitées à obtenir communication du bulletin n° 2 du casier judiciaire et en précisant celles des informations qui, enregistrées au casier judiciaire national, ne peuvent figurer sur ce bulletin n° 2, le législateur a entendu faire bénéficier, dans certaines circonstances et après un délai d'épreuve, certains condamnés d'un « droit à l'oubli » opposable aux administrations de l'Etat. Dans ces conditions, l'éventualité qu'un fichier de police judiciaire, quelle qu'en soit la nature, puisse être consulté dans le cadre d'enquêtes administratives de moralité, priverait d'effet les dispositions légales des articles *775* et suivants du code de procédure pénale qui énumèrent les condamnations dont la mention est exclue ou peut être effacée du bulletin n° 2 et les conditions dans lesquelles les juridictions pénales peuvent prononcer, dans le souci de faciliter la réinsertion sociale des personnes, la non inscription d'une condamnation au bulletin n° 2 du casier judiciaire.

2.3. Les consultations du STIC seront subordonnées à une habilitation individuelle des personnels de police judiciaire concernés et feront l'objet d'un enregistrement systématique à des fins de contrôle.

Afin de prévenir toute utilisation du STIC à des fins étrangères à ses finalités, une procédure d'habilitation individuelle sera mise en place, ces habilitations étant délivrées par les chefs de service. Seules les personnes ainsi habilitées pourront consulter les informations enregistrées et un système de journalisation des interrogations permettra de conserver trace pendant trois ans du matricule de tout fonctionnaire du ministère de l'Intérieur ayant consulté le STIC, de l'identité du fonctionnaire associée à ce matricule, du service auquel il appartient, de l'identification du terminal utilisé, des dates et heures de connexion, des critères de recherche utilisés et du nombre de réponses obtenues.

De même, toute mise à jour (création, modification, suppression) provoquera l'enregistrement pendant trois ans des informations relatives au fonctionnaire de police qui y aura procédé.

Il convient de relever que les historiques horodatés des données de consultation du STIC seront tenus à la disposition de la Commission, comme l'a confirmé le ministère de l'Intérieur. Il convient de relever en outre que toute connexion au fichier provoquera l'affichage d'une page écran informant ses utilisateurs que les données de connexion permettant d'identifier les interrogations du fichier et leur auteur seront conservées à des fins de contrôle.

Ces dispositifs de sécurité devraient prévenir toute utilisation abusive ou illicite du fichier. Il conviendrait cependant, pour leur assurer une complète efficacité, que l'ensemble des fonctionnaires de police concernés en soient informés par voie de circulaire, laquelle devrait rappeler, notamment, que

toute consultation du fichier à des fins étrangères aux finalités mentionnées dans le projet de décret constituerait le délit de détournement de finalité prévu et réprimé par l'article 226-21 du code pénal d'une peine de cinq ans d'emprisonnement et de 2 000 000 de francs d'amende.

2.4. Il convient de renforcer ces mesures en prévoyant que le gestionnaire du fichier devra rendre compte chaque année à la CNIL de ses activités de vérification, de mise à jour et d'effacement des informations. Ce compte rendu annuel devra notamment préciser le nombre de personnes fichées au titre des « mis en cause » et le nombre de personnes fichées au titre de « victimes », le nombre d'informations qui auront été complétées à la suite de la notification de certaines décisions judiciaires par les procureurs de la République ainsi que le nombre d'informations qui auront été effacées. Le projet de décret devra être complété en ce sens.

3. Catégories d'informations traitées et données sensibles

Les catégories d'informations enregistrées sont, s'agissant des mis en cause, l'identité et le cas échéant l'alias, les date et lieu de naissance, la situation familiale, la filiation, la nationalité, l'adresse et la profession, l'état de la personne selon une nomenclature définie par le ministère de l'Intérieur, son signalement et sa photographie. S'agissant des victimes, les catégories d'informations enregistrées sont l'identité, les date et lieu de naissance, la situation familiale, la nationalité, l'adresse, la profession, l'état de la personne. La Commission prend note que seul le signalement et la photographie des personnes disparues et des corps non identifiés sont enregistrés.

Certaines informations peuvent directement ou indirectement relever des données sensibles énumérées par l'article 31 de la loi du 6 janvier 1978 qui subordonne leur collecte et leur enregistrement à un motif d'intérêt public. La finalité du fichier justifie qu'il soit fait application des dispositions du 3e alinéa de l'article 31 de la loi à la condition que la portée de la dérogation soit circonscrite aux seules informations qui résultent de la nature ou des circonstances de l'infraction ou à celles qui se rapportent à des signes physiques particuliers, objectifs et permanents en tant qu'élément de signalement des personnes dès lors que ces éléments de signalement sont nécessaires à la recherche et à l'identification des auteurs d'infraction. Il y a lieu de compléter en ce sens le projet de décret.

4. Durée de conservation des informations

Le projet de décret précise que les données concernant les personnes majeures mises en cause seront, en principe, conservées vingt ans à compter de la date d'établissement de la procédure. Toutefois, les informations concernant certains crimes et délits figurant sur une liste annexée au décret seront conservées pendant quarante ans. En tout état de cause, les données relatives aux personnes âgées de plus de *75* ans seront systématiquement supprimées du fichier.

Par dérogation à ces règles, les informations relatives aux six catégories de contraventions de cinquième classe, aux délits routiers, aux délits d'abandon de famille et de non représentation d'enfant et aux délits d'usage de stupéfiant seront conservées pendant cinq ans.

S'agissant des mineurs, et conformément à la demande qui avait été faite par la Commission, le projet de décret prévoit que la durée de conservation de principe est de cinq ans, exception faite de certains crimes et délits graves énumérés dans deux listes annexées au décret, qui déterminent des durées de conservation, respectivement, de dix et vingt ans.

Le projet de décret prévoit, enfin, s'agissant des personnes mises en cause, que, dans l'hypothèse où une nouvelle infraction serait commise avant l'expiration de ces durées, l'ensemble des informations enregistrées serait alors conservé pendant le délai le plus long.

La durée de conservation des informations concernant les victimes est au maximum de quinze ans, cette durée pouvant être prolongée jusqu'à la découverte des objets lorsque l'infraction porte sur des œuvres d'art, des bijoux ou des armes. Toutefois, toute victime pourra demander la suppression des informations qui la concernent dès lors que l'auteur de l'infraction aura été définitivement condamné.

Dans leur principe, de telles durées paraissent, dès lors que les informations enregistrées seront mises à jour ou effacées selon les règles précédemment définies, justifiées par la finalité de recherche et d'identification des auteurs d'infractions. Elles appellent cependant deux réserves.

La première réserve porte sur la durée de conservation (vingt ans) de certaines infractions qui ne paraît pas justifiée par la finalité de recherche et d'identification criminelle. Tel est le cas pour les infractions involontaires (articles 221-6 et 222-19 du code pénal), les infractions de détournement de gage ou d'objet saisi (articles 314-5 et 314-6 du code pénal), le vol simple (article 311-3 du code pénal), le délit d'entrave aux libertés protégées (article 431-1 du code pénal) et l'infraction de participation sans arme à un rassemblement interdit (article 431-4 du code pénal). Compte tenu de la nature de ces infractions, des conditions dans lesquelles elles sont généralement constatées et des pénalités qui leur sont associées, la durée de conservation des informations s'y rapportant, fixée à vingt ans, paraît excessive au regard des finalités du traitement et doit être ramenée à cinq ans. Le projet de décret doit être modifié en ce sens.

La deuxième réserve concerne les infractions dites de « trafics » mentionnées aux annexes I et III qui déterminent respectivement des durées de conservation dérogatoires de quarante ans pour les majeurs (au lieu de vingt) et de vingt ans pour les mineurs (au lieu de cinq). La Commission relève qu'à la différence des autres infractions énumérées dans ces annexes, le « trafic » ne constitue pas une qualification pénale autonome, hors le cas du trafic de stupéfiants, visé par ailleurs. Compte tenu des observations et propositions nouvelles faites par le commissaire du gouvernement auprès de la CNIL tendant à substituer à la rubrique « trafic » la référence au crime de « vol en bande organisée », la Commission prend acte de cette modification. Les annexes I et III devront être modifiées en conséquence.

5. Droit d'accès.

Le projet de décret prévoit que le droit d'accès s'exercera dans les conditions prévues par l'article 39 de la loi du 6 janvier 1978. Toutefois, la CNIL pourra constater, en accord avec le ministère de l'Intérieur, et après accord du procureur de la République concerné, sous réserve que la procédure soit judiciairement close, que les informations nominatives enregistrées ne

mettent pas en cause la sûreté de l'Etat, la défense ou la sécurité publique et qu'il y a donc lieu de les communiquer à la personne intéressée.

Ce dispositif qui permettra, dans ces conditions, aux personnes d'avoir directement connaissance des informations les concernant constitue une garantie nouvelle de nature à renforcer les droits qui leur sont reconnus à l'égard d'un fichier informatique de cette nature.

6. Conditions de consultation du fichier à des fins de police administrative et de sécurité

Le projet de décret prévoit que les informations enregistrées dans le STIC pourront être consultées, dans certaines conditions, dans le cadre de missions de police administrative ou de sécurité, 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. Dans de tels cas, et par dérogation aux dispositions de l'article R. 156 du code de procédure pénale, les informations figurant dans le STIC pourraient être consultées sans autorisation du procureur de la République ou du procureur général par des personnels de la police nationale individuellement désignés et spécialement habilités par le directeur général de la police nationale ou par le préfet.

Bien que l'éventualité de telles consultations soit étrangère aux finalités de police judiciaire du STIC, elle peut être admise dès lors que la sécurité des fonctionnaires de la police nationale ou la sécurité des tiers est susceptible d'être mise en danger dans des circonstances particulières. Tel peut être le cas à l'occasion de certaines interventions en urgence, que celles-ci relèvent d'une mission de police judiciaire ou d'une mission de police administrative, ainsi que dans les circonstances où le déroulement d'un événement public exceptionnel commande que toutes précautions soient prises pour assurer la sécurité des personnes.

Un tel usage du fichier ne saurait cependant porter atteinte au secret de l'enquête et de l'instruction garanti par les dispositions de l'article 11 du code de procédure pénale. Aussi, de telles consultations ne doivent-elles concerner que des informations relatives à des procédures judiciairement closes. En outre, un tel usage du fichier doit être strictement encadré. H y a lieu sur ce point de prendre acte que le ministère de l'Intérieur a prévu que les personnels concernés devraient être individuellement habilités à consulter le fichier par le directeur général de la police nationale ou par le préfet et qu'en aucun cas la consultation du fichier à de telles fins ne permettra d'accéder aux informations nominatives relatives aux victimes ou aux personnes ayant bénéficié d'une décision judiciaire en leur faveur. Enfin, les procédures de journalisation des consultations du fichier à de telles fins s'appliqueront dans les mêmes conditions que pour la police judiciaire.

Il convient de renforcer ces garanties en instaurant un double degré d'interrogation du STIC, le premier niveau permettant d'obtenir comme seule réponse connu », « inconnu », l'interrogation s'effectuant uniquement sur les personnes enregistrées au titre de « mis en cause », le deuxième niveau, réservé à un nombre limité de responsables opérationnels, permettant d'obtenir des informations concernant les affaires dans lesquelles la personne a été mise en cause.

7. Gestion des archives

Le projet de décret mentionne au titre des finalités la rationalisation du recueil et de l'exploitation des informations contenues dans les procédures établies par les services de police aux fins, notamment, de gestion des archives. Si le STIC doit permettre, pendant la durée de conservation des informations, d'identifier le service qui détient le dossier de la procédure, en tout état de cause, à l'expiration des délais de conservation fixés par le projet de décret, les informations directement ou indirectement nominatives concernées devront être supprimées, les dossiers de procédure correspondant étant régis par l'article 4-1 de la loi du 3 janvier 1979 modifiée par la loi du 12 avril 2000. Le souci d'éviter toute ambiguïté doit conduire à supprimer à l'article premier du projet de décret la référence faite à la gestion des archives.

8. Information des personnes

Il convient que les personnes concernées soient clairement et précisément informées de leurs droits et tout particulièrement de leur droit d'accès, de leur droit de demander que la qualification judiciaire des faits soit substituée, le cas échéant, à la qualification initiale telle qu'elle est enregistrée dans le STIC, ainsi que du droit de s'adresser au procureur de la République territorialement compétent pour solliciter la mise à jour des informations les concernant. Le ministère de l'Intérieur et le ministère de la Justice devront informer la Commission des mesures prises à cet effet.

Émet un avis conforme au projet de décret sous les réserves suivantes :

— **à l'article premier :**

— au premier alinéa, supprimer les mots « la rationalisation du recueil et de » et « de gestion des archives »,

— supprimer le deuxième alinéa,

— au troisième alinéa, supprimer les mots « et notamment toutes informa tions nominatives concernant les » et les remplacer par les mots « dans les seuls cas où ces informations résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs d'infractions définies à l'article 2 » ;

— **à l'article 2 :**

— rédiger ainsi qu'il suit à la fin de cet article, après les mots « mentionnées au premier alinéa de l'article premier ci-dessus » : « lorsqu'elles concernent des personnes à l'encontre desquelles sont réunis lors de l'enquête prélimi naire, de l'enquête de flagrance ou sur commission rogatoire des indices ou des éléments graves et concordants attestant leur participation à la commis sion d'un crime, d'un délit ou d'une contravention de cinquième classe prévue aux articles R 625-1, R 625-7, R 625-8, R 635-1, R. 645-1 et R 645-12 du code pénal, ou les victimes de ces infractions » ;

— ajouter un deuxième alinéa ainsi rédigé : « Les informations nominatives relatives aux personnes mises en cause et aux victimes ainsi que la qualifica tion des faits, telles qu'elles sont enregistrées dans le STIC, sont transmises au procureur de la République territorialement compétent en même temps que la procédure » ;

— **à l'article 3 :**
— compléter le deuxième alinéa ainsi qu'il suit : « Les informations directement ou indirectement nominatives relatives aux personnes mises en cause sont supprimées par le gestionnaire du fichier en cas de décision de relaxe ou d'acquittement devenue définitive. Les informations directement ou indirectement nominatives relatives aux personnes ayant bénéficié d'un non-lieu font l'objet d'une mise à jour, sauf dans le cas où le procureur de la République territorialement compétent en prescrit l'effacement. Les informations directement ou indirectement nominatives relatives aux personnes mises en cause sont complétées par les décisions de classement sans suite motivées par l'insuffisance de charges à l'encontre des personnes concernées ».
— au quatrième alinéa, après les mots « d'une enquête préliminaire, de flagrance » insérer les mots « ou sur commission rogatoire d'une juridiction d'instruction » ;
— ajouter un alinéa ainsi rédigé : « Toute personne ayant bénéficié d'une mesure de classement sans suite visée au deuxième alinéa, d'une décision judiciaire de non-lieu, de relaxe ou d'acquittement devenue définitive peut demander au procureur de la République territorialement compétent, soit directement, soit par l'intermédiaire de la CNIL à l'occasion de l'exercice de son droit d'accès, que le fichier soit mis à jour dans les conditions prévues au deuxième alinéa de l'article 3 compte tenu de ces suites judiciaires » ;
— **supprimer l'article 5** (par coordination avec la modification apportée à l'article 2) :
— **à l'article 6 :**
— remplacer les mots « les autorités judiciaires » par les mots « les magistrats du Parquet » ;
— ajouter un nouvel alinéa ainsi rédigé : « Seules celles des informations enregistrées dans le STIC qui sont relatives à la procédure en cours peuvent être jointes au dossier de la procédure » ;
— **rédiger l'article 7 ainsi qu'il suit :** « Par dérogation aux dispositions de l'article R 156 du code de procédure pénale, les informations figurant dans le traitement qui se rapportent à des procédures judiciairement closes, à l'exception des données complétées par les informations transmises par le procureur de la République en application de l'alinéa 2 de l'article 3 et des données relatives aux victimes, peuvent être consultées sans autorisation du procureur de la République ou du procureur général dans le cadre de missions de police administrative ou de sécurité, 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. La consultation du STIC est alors réservée aux personnels de la police nationale individuellement désignés et spécialement habilités par le directeur général de la police nationale ou par le préfet. L'habilitation comporte deux niveaux d'accès. Elle précise le niveau qui est conféré à son titulaire par l'autorité compétente » ;
— **à l'article 8.I** (premier tiret) il est inséré après les mots « 227-3 à 227-11 », les mots «221-6, 222-19, 311-3, 314-5, 314-6, 431-1 et 431-4» ;
— **un article nouveau** est inséré après l'article 10 ainsi rédigé : « Sans préjudice de l'application de l'article 21 de la loi du 6 janvier 1978 susvisée, la direction générale de la police nationale rend compte chaque année à la Commission nationale de l'informatique et des libertés de ses ac-

tivités de vérification, de mise à jour et d'effacement des informations enregistrées dans le traitement. »

— **aux annexes I et III,** la référence faite aux « Trafics (véhicules, or et métaux précieux, bijoux, armes) » est supprimée, et remplacée par « vol en bande organisée ».

Chapitre 4

LES CONTRÔLES D'ACCÈS PAR BIOMÉTRIE

I. QUELQUES OBSERVATIONS GÉNÉRALES SUR LA 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).

Les finalités des techniques biométriques sont très diverses

Les plus courantes sont les finalités de vérification et d'authentification ainsi que les finalités d'identification. Mais ces finalités ne sont pas du même ordre. S'agissant des finalités de vérification et d'authentification, il peut être recouru aux techniques biométriques sans qu'il soit nécessaire de collecter d'autres données directement ou indirectement nominatives. La vérification ne se soldera que par un « jeton » de type oui/non permettant d'accéder à tel type de service. ◦ titre d'exemple, le centre de loisir de Disneyland (Floride) recourt à une application biométrique fondée sur la géométrie de la main qui n'a nullement pour objet d'identifier les visiteurs mais d'établir si un visiteur a ou non le droit d'accéder à tel ou tel service de loisir du parc. L'application est tout à fait anonyme. Les systèmes de reconnaissance à base d'empreintes digitales qui peuvent être « embarqués » sur des PC portables, des téléphones mobiles ou des assistants numériques de poche sont, dans de nombreux cas, à classer dans cette catégorie. En effet, l'activation par l'utilisateur de

fonction comportant des éléments d'identification demeure placée sous le seul contrôle de la personne concernée et ne suppose pas la constitution d'une base de données d'éléments d'identification biométrique.

Il en va tout autrement des systèmes d'identification qui nécessitent l'enregistrement préalable de l'élément biométrique utilisé dans une base de données afin d'identifier, par les techniques de reconnaissance, chaque personne concernée. Il s'agira par exemple de contrôler l'accès à des locaux et de veiller à ce que seules les personnes préalablement habilitées puissent y avoir accès ou encore de systèmes de plus en plus fréquemment utilisés pour le contrôle des horaires.

Une dernière finalité mérite d'être citée, tant elle pourrait être appelée à se développer : la cryptographie biométrique. Dans ce cas, il s'agirait d'utiliser la biométrie sans stocker d'éléments de comparaison dans une base de données (on parlera alors de « gabarit »), pour crypter des données, c'est-à-dire assurer leur confidentialité. Ce type de systèmes est actuellement à l'étude, notamment en matière de cartes bancaires pour remplacer le code PIN des cartes bancaires ; l'élément biométrique choisi ou, pour plus exactement parler, son « gabarit » jouera le rôle du code PIN : il ne sera pas transmis mais ouvrira seulement, et avec plus de certitude, les fonctionnalités reconnues comme étant demandées par le titulaire des droits.

Il résulte de ces observations que toute utilisation des technologies biométriques ne repose pas sur la constitution préalable d'une base de données.

La diversité des données biométriques

On songe souvent, évidemment, à l'empreinte digitale. Mais le contour de la main, la reconnaissance des visages, la reconnaissance vocale, la reconnaissance par la rétine — laquelle est tout à fait différente de la reconnaissance par l'iris, la reconnaissance de la dynamique d'une signature sont autant d'éléments biométriques autour desquels se développent des technologies et certaines applications. Sans doute, l'empreinte digitale présente-t-elle, à la différence d'autres caractéristiques, une spécificité : elle est le seul élément biométrique qui soit omniprésent : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence : les objets que l'on touche (un verre, une table, une lampe de chevet, etc.) mais également désormais un vêtement, c'est-à-dire des objets à surface non lisse. ◦ cet égard, l'empreinte digitale est presque aussi redoutable que les traces ADN.

La diversité des technologies biométriques

De nombreux procédés biométriques commercialisés ne sont pas considérés comme suffisamment fiables pour discriminer une personne d'une autre ; aussi, malgré les argumentaires développés par les industriels du secteur, doit-on le plus souvent associer la biométrie à un mot de passe ou à une carte magnétique ou à puce. Dans le souci d'améliorer l'authentification de l'utilisateur, les organismes ont par ailleurs tendance à cumuler différents procédés : ainsi, la reconnaissance du visage et des empreintes vocales ou alors, sur un clavier d'ordinateur, un mot de passe, son

empreinte digitale et une carte à puce. Dans ce dernier cas, on trouve alors un triple niveau d'authentification : par ce que l'on sait, par ce que l'on possède et par ce que l'on est : c'est ce que l'on appelle la biométrie multimodale. Evidemment, la combinaison technique biométrique et mot de passe demeure la moins coûteuse, mais c'est l'association de la carte à puce et de la technologie biométrique qui présenterait incontestablement les plus grands avantages pratiques et économiques. Les avantages d'une telle association sont au demeurant considérables en termes de protection des données personnelles et des libertés individuelles dans la mesure où il n'est plus alors besoin de base de données biométriques, « l'empreinte biométrique » demeurant sur soi, au coeur de la carte à puce.

L'intérêt de mener une étude approfondie sur la recherche fondamentale et appliquée en cette matière a d'ailleurs conduit la CNIL à entreprendre, en liaison avec les professionnels concernés, une étude d'ensemble de ces questions sous l'éclairage de la protection des données personnelles et de la vie privée. Il convient cependant de constater, à cet égard, que les applications dont la CNIL a été saisie durant l'année, ont plutôt cumulé les difficultés dans la mesure où elles prévoyaient à la fois le recours à l'empreinte digitale, donnée biométrique tout à fait spécifique, et la constitution de base de données de comparaison, ce qui soulevait légitimement certaines interrogations au regard des libertés individuelles et publiques. C'est ce cumul-là qui a conduit la Commission à rendre une série d'avis particulièrement rigoureux dont il est rendu compte dans le présent rapport d'activité.

II. LES PROBLEMES SPECIFIQUES LIES › LA CONSTITUTION DE BASE DE DONNÉES D'EMPREINTES DIGITALES

L'empreinte digitale : une biométrie chargée d'histoire

Les chinois de la dynastie Tang (618-906) sont généralement considérés comme les premiers ayant utilisé l'empreinte digitale pour authentifier les contrats, méthode qui a été reprise en 1858 dans un district des Indes britanniques par Sir William Herschel pour authentifier les contrats passés avec les hommes d'affaires indigènes. Mais ce n'est qu'à partir de 1892, avec Sir Francis Galton, statisticien, cousin de Darwin, que l'utilisation de l'empreinte digitale reçut une base scientifique avec la démonstration qu'elle était unique pour chaque individu et ne changeait pas au cours d'une vie. Edward Henry, administratif du Bengale, donna un caractère opératoire aux observations de Galton en élaborant un système de classification des empreintes. Le succès aux Indes fut tel en 1897 pour l'identification des criminels, que New Scotland Yard adopta ce procédé à partir de 1901, date à laquelle Henry était nommé à la tête du nouveau bureau des empreintes digitales. Ensuite, le procédé se diffusa très rapidement dans des laboratoires de police scientifique du monde entier dont la France, en 1903, grâce à Alphonse Bertillon, déjà célèbre pour avoir fait adopter l'anthropométrie par l'ensemble des polices françaises dès 1882.

Des centaines de millions d'empreintes ont ainsi été collectées et traitées manuellement pendant plus d'un demi-siècle avant que l'on assiste aux premiers balbutiements de l'informatique. C'est cet usage policier qui a imposé sa norme technique dans la façon de traiter l'empreinte du doigt.

Mais cette paternité policière ne constituerait pas un problème particulier si, en elle-même, toute base de données enregistrant les empreintes digitales des personnes concernées, quelle que soit la finalité poursuivie, n'était pas, au moins potentiellement, un outil nouveau mis à la disposition de la police et s'ajoutant aux traditionnels fichiers dont elle dispose. Songeons par exemple que les Philippines ont mis en œuvre une base de données d'empreintes digitales destinée à identifier les personnes susceptibles de solliciter une aide sociale comportant... 20 millions d'empreintes !

Les bases de données d'empreintes digitales en France

La Commission a eu connaissance de plusieurs traitements d'informations nominatives reposant sur la collecte d'empreintes digitales ou la reconnaissance d'un individu par ses empreintes digitales. Tel a été le cas pour le fichier national des empreintes digitales (FNAED) mis en œuvre par le ministère de l'Intérieur en matière criminelle (délibération. n° 86-102 du 14 octobre 1986 — rapport annuel 1986 p. 342) et pour le fichier mis en œuvre par l'OFPRA en matière de contrôle et de gestion des demandes d'asile (délibération n° 87-106 du 3 novembre 1987 — rapport annuel 1987 p. 213). Mais il s'agissait là d'applications par nature policière, qu'il s'agisse de police administrative ou de police judiciaire.

Ce n'est que plus récemment que la CNIL a été saisie d'applications de reconnaissance par empreintes digitales au titre du contrôle d'accès.

Le premier dossier qu'elle avait examiné concernait la Banque de France qui souhaitait recourir à un dispositif de reconnaissance par empreintes digitales pour l'accès à des zones hautement sécurisées. Par délibération n° 97-044 du 10 juin 1997 (rapport annuel 1997 p. 288), la CNIL a donné un avis favorable à la mise en œuvre de ce traitement.

Au cours de l'année 2000, plusieurs dossiers ont permis à la Commission de préciser sa doctrine en matière d'utilisation de dispositifs biométriques, qui ont vocation à se développer considérablement au cours des prochaines années.

D'après les chiffres avancés par les professionnels, le marché de la biométrie couvre actuellement 100 millions de personnes dans le monde avec une longueur d'avance pour les systèmes d'empreintes digitales (30 % des systèmes mis en œuvre), suivis de très près par les systèmes de reconnaissance du contour de la main (27%).

Les mécanismes de base de la biométrie consistent tout d'abord à « enrôler » la personne, c'est-à-dire à stocker les éléments permettant de la reconnaître. Il s'agira ensuite soit de l'authentifier (le système compare la nouvelle signature avec celle qui a précédemment été enregistrée et reconnaît la personne comme celle qui a

été enrôlée), soit de l'identifier (le système identifie tel élément biométrique comme propre à tel individu).

Ce qu'apporte la biométrique, c'est une meilleure authentification/identification, selon le choix effectué, des personnes que l'on veut contrôler. La personne doit en effet présenter une partie d'elle-même (l'un de ses doigts, une paume de la main, son œil, sa voix en prononçant une phrase) à l'équipement de contrôle. Les taux de reconnaissance sont souvent au-dessus de 90 %, même pour des systèmes à bas prix. Les algorithmes de traitement, combinés à des micros de plus en plus performants, se sont en effet beaucoup perfectionnés durant les années 90, d'où des produits de meilleure qualité. Ainsi, si un employé présente la paume de sa main légèrement enflée par rapport à l'état de sa main telle qu'elle avait été initialement enregistrée, le logiciel peinera probablement pour faire la reconnaissance, mais la fois suivante, si l'employé représente sa main toujours enflée, la reconnaissance sera immédiate.

Un algorithme de reconnaissance biométrique ne donne jamais le même résultat quand une même personne se présente deux fois de suite, car les conditions du contrôle ne peuvent jamais être identiques (voix légèrement différente, doigt posé différemment). Les logiciels sont donc toujours conçus pour fournir une réponse sous la forme d'un pourcentage de coïncidences : « par rapport à ce que j'ai dans ma base de données, il y a x % de coïncidences avec Dupont, y % avec Durand, etc. ».

Celui qui obtient le meilleur « score » n'est pas pour autant nécessairement retenu, tout dépend de la politique « sécuritaire » choisie par l'entreprise. Illustrons ce propos par l'exemple caricatural suivant. Supposons que l'entreprise n'a que deux employés, Dupont et Durand, et que le système de contrôle réponde : « il y a 30 % de ressemblance avec Durand et 10 % avec Dupont ». Le choix pourrait être : « malgré son faible résultat de 30 %, ce ne peut être que Durand et on l'accepte ». L'autre choix pourrait être : « le pourcentage est vraiment trop faible, on ne retient personne ». Ainsi, en paramétrant le logiciel de reconnaissance, le responsable de la mise en œuvre définit implicitement deux taux : le taux de faux rejets (TFR), pourcentage de personnes rejetées par erreur, et le taux de fausses acceptations (TFA) qui est le pourcentage d'acceptations qui n'auraient pas dû être retenues.

Mais incontestablement l'empreinte digitale et le contour de la main sont les deux données biométriques les plus utilisées à l'heure actuelle.

La technique de reconnaissance par empreintes digitales

Une empreinte digitale est faite d'une série de crêtes et de sillons (creux) tracés sur la surface du doigt.

Dans les applications judiciaires, la qualité de l'empreinte est essentielle aussi utilise-t-on une technique particulière de collecte basée sur un lecteur optique : le doigt est d'abord posé sur un système optique (un prisme) et son image optique est ensuite traitée pour fournir une image informatique, c'est-à-dire une numérisation, comme le ferait un scanner.

Dans les applications commerciales où l'on cherche à diminuer les coûts et l'encombrement, l'image est obtenue par des capteurs placés en contact direct avec le doigt et qui, par la mesure d'une certaine propriété physique ou la distance les séparant de la surface du doigt, décèlent les crêtes ou les sillons (par exemple, le FingerChip de Thomson — Thalès aujourd'hui — mesure les différences thermiques existant entre les crêtes et les creux).

Quel que soit l'appareillage de départ, le résultat final est une image informatique de l'empreinte digitale.

C'est à ce stade qu'entre en jeu le logiciel.

En effet, si l'être humain, par l'intelligence qui lui est propre, « voit » immédiatement dans une image le dessin formé par les crêtes et les sillons, l'ordinateur lui, de prime abord, ne voit qu'un nuage de points. ◦ partir de ce constat, deux approches s'affrontent. La première, la technique des minuties, essaie de reconstituer grossièrement la forme des crêtes et des sillons. La deuxième, la méthode des corrélations, ne se préoccupe pas des crêtes et sillons : elle fait une analyse globale du nuage de points pour en définir ses caractéristiques mathématiques.

Ce qui est intéressant de noter, à ce stade, c'est qu'une fois l'extraction logicielle terminée, par les minuties ou par l'analyse par corrélations, l'image informatique de l'empreinte n'est plus utile.

Dans la technique des minuties, pour obtenir le tracé des crêtes, on se contente de rechercher les points remarquables situés sur ces lignes, les endroits où apparaît soit une bifurcation soit une terminaison. Par analogie, c'est comme si pour le tracé d'un parcours en voiture, on ne retenait que les endroits où se produit un changement de direction, soit à gauche soit à droite. Ces points remarquables sont appelés les minuties.

Le calcul montre qu'avec un nombre restreint de minuties (15 ou 20) correctement localisées, il est possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.

L'objectif est donc d'avoir un minimum de 15 minuties de bonne qualité. Pour arriver à ce score, l'algorithme de reconnaissance de forme doit commencer par sélectionner un échantillon plus large, une centaine de minuties potentielles. Beaucoup d'entre elles s'avéreront par la suite de fausses minuties. D'autres seront des minuties éliminées pour leurs mauvaises qualités.

En moyenne, avant compactage et compression finale, chaque minutie est mémorisée sur environ 16 octets (caractères), ce qui donne un fichier de 240 octets pour 15 minuties. Après compactage et compression, on peut descendre à une centaine d'octets. C'est ce fichier qui est appelé la « signature » de l'empreinte.

Pour préparer les recherches futures et minimiser les temps consacrés à l'identification, chaque nouvelle empreinte doit être indexée dans la base de données avec le maximum d'exactitude, par des classements successifs dans des catégories pré-établies, du plus général au moins général, à la manière des poupées russes. La qualité première que doit posséder un système de classement d'empreintes

digitales est d'être peu sensible aux translations, rotations et déformations qui affectent souvent la prise des empreintes digitales : si deux « signatures » calculées à partir du même doigt mais à partir de deux prises d'empreinte différentes ne donneront jamais 100 % de ressemblance du fait des différences inévitables qui existent lors de l'acquisition des deux images (le doigt n'est pas placé sur l'appareil exactement de la même façon, soit un peu plus au fond (translation), un peu plus de biais (rotation), ou un peu plus écrasé sur l'un des côtés (déformation)), elles devront toujours fournir un niveau élevé de similitude.

La technique des minuties a le défaut d'être sensible à la mauvaise qualité de l'empreinte digitale car les minuties seront alors difficiles à repérer. Également, elle ramène l'ensemble de l'empreinte à 15-20 minuties et ne prend pas en compte le dessin général des crêtes et sillons de l'empreinte.

Le problème spécifique de l'empreinte digitale

Si, historiquement, le marché de l'empreinte est policier, le second segment de marché concerne les cartes d'identité. De nombreux pays sans état civil fiable, déstabilisés par des vagues migratoires importantes, notamment en Afrique, ont recours à la technique de l'empreinte (Nigeria) pour gérer la délivrance des cartes nationales d'identité. On peut également citer le cas de la Malaisie ou tout récemment du Kosovo.

Le troisième segment de marché concerne les contrôles d'accès. Les concepteurs de système espèrent que ce marché se développera en France d'une part du fait de la loi sur les 35 heures et de ses conséquences en termes de gestion des horaires des salariés et, d'autre part, de l'accentuation de la mobilité (on parle désormais de « m-commerce ») qui rend nécessaire l'authentification des personnes. Ainsi, la « bio-reconnaissance » est-elle présentée comme l'avenir du paiement électronique.

L'empreinte digitale aurait donc vocation à s'éloigner de la police — c'est en tout cas ce que mettent en valeur les concepteurs de systèmes de reconnaissance d'empreintes digitales. Ils exposent généralement certains de leurs succès, tels que le recours à l'empreinte digitale pour le versement d'allocations sociales dans des pays comme les Etats-Unis, le Mexique. Cependant, le tropisme policier n'est pas loin. Ainsi, en matière de gestion de personnel, les employeurs font valoir que le recours à la biométrie permet de traiter automatiquement les horaires d'entrée et de sortie, en présentant l'avantage d'interdire toute possibilité de biaiser avec le système de pointage. L'empreinte interdit alors à un salarié de remettre son badge à un collègue...

La forte connotation policière qui est attachée à l'empreinte digitale s'estompera peut être à l'avenir. Ainsi, au Royaume-Uni, il semblerait que des collèges utilisent ce système pour contrôler les accès de même que des clubs privés en Belgique. En Finlande, des bibliothèques utiliseraient la reconnaissance des empreintes digitales pour gérer le système de prêt d'ouvrages.

Cependant, cette connotation policière demeure. Ainsi, en France, dans les années 1980, des commerçants qui, soucieux de prévenir le phénomène des chèques volés ou impayés, demandaient à leurs clients d'apposer leur empreinte au dos

des chèques remis en paiement, avaient dû renoncer à cette pratique devant l'émoi suscité par cette initiative, alors même qu'elle n'avait guère qu'une portée symbolique, ne pouvant être en pratique d'aucune efficacité.

Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale. Il pourrait presque être soutenu que l'empreinte digitale est aux autres données biométriques ce que le NIR est aux autres données personnelles : une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers. C'est la grande différence entre cette donnée biométrique et toutes les autres.

C'est ainsi que le ministère de l'Intérieur n'a pas donné suite au projet de numérisation du relevé des empreintes digitales qui sont prises à l'occasion de la demande d'une carte nationale d'identité, afin de ne pas donner l'impression que pourrait se constituer, à l'occasion d'une démarche administrative, un outil de police judiciaire.

Dans le souci d'écarter cet argument, certains opérateurs n'hésitent pas à mettre en avant l'incompatibilité de leur système avec celui employé par la police. Ils font valoir que leur modèle n'est pas une empreinte digitale au sens de la collection des minuties recueillies par la police et qu'il serait impossible de fabriquer cette empreinte digitale à partir du profil de doigt réalisé par leur système.

Les efforts consentis par ces sociétés pour que les bases de données qu'elles constituent ne puissent en aucun cas être utilisées à des fins étrangères à leur finalité initiale sont du plus grand intérêt et méritent d'être plus amplement étudiés. Mais les arguments qu'elles donnent n'ont pas tous la même valeur. Ainsi, le fait que la base de données ne soit pas une base de données d'images et ne puisse pas être comparée avec une base de données policière est indifférent. Le problème est de savoir si une empreinte relevée sur un verre, une table, un téléphone peut ou non être comparée, une fois analysée, y compris par l'étude des minuties, avec les éléments de référence inclus dans le fichier de ces entreprises.

C'est moins l'empreinte digitale qui fait problème, que le stockage d'une numérisation de cette empreinte, que l'information se présente comme une image ou sous la forme d'un code ou d'un numéro. ◦ cet égard, la solution consistant à ce que les profils des doigts soient consignés non dans une base de données mais soient éclatés sur les supports à protéger (ordinateur central, PC, carte à puce...) et non conservés dans une base de données unique paraîtrait bien préférable.

III. L'ACCES AUX CANTINES SCOLAIRES

Les services de la Commission ont eu connaissance de la mise en œuvre du traitement à la suite d'une démarche de l'administration du collège désireuse de se mettre en conformité avec la loi du 6 janvier 1978.

Dès réception de la demande d'avis, une mission d'information sur place a été menée, le concepteur du produit n'ayant pas caché son souhait de le diffuser largement dans le secteur de l'éducation et 60 établissements scolaires ayant déjà manifesté de l'intérêt pour ce produit.

Le traitement devait permettre de gérer l'accès des élèves et des personnels enseignants et administratifs de l'établissement à la cantine scolaire. Environ 350 personnes étaient concernées par le traitement qui comportait deux bases de données, gérées de manière distincte :

— un fichier de gestion exploité par le service de l'intendance pour la facturation,

— une base de données biométriques comportant une représentation codée des em preintes digitales de chaque personne.

Les motivations avancées par les concepteurs et les utilisateurs pour expliquer le choix de la biométrie concernent l'aspect sécurité et confort. Plus besoin de manipuler des cartes, de gérer l'octroi de mots de passe...

En l'espèce, l'administration du collège a indiqué que l'utilisation dudit système permet de supprimer toute manipulation d'argent à l'intérieur de l'établissement et de ne plus gérer les problèmes de cartes oubliées, perdues ou volées qui alourdissaient les tâches de gestion. Avec le système antérieur, l'intendance devait gérer quotidiennement 50 cas de cartes oubliées ou perdues. Il a également été avancé que toutes les tentatives de fraude, certains collégiens tentant de manger deux fois, étaient mises en échec du fait de la fiabilité du système (sic !).

La Commission a rendu un avis défavorable à la mise en œuvre du traitement en se fondant sur le caractère excessif qu'il revêtait au regard de la finalité poursuivie. En effet, si la constitution des bases de données d'empreintes digitales peut être justifiée dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse, la CNIL demeure, jusqu'à présent en tout cas, réservée à l'égard de la généralisation de telles bases de données dans la mesure où, compte tenu des caractéristiques propres aux empreintes digitales, la conservation dans un traitement des empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité que son concepteur lui avait initialement assignée. En effet, et à la différence d'autres données biométriques, telles que le contour de la main, l'iris ou la reconnaissance vocale, les empreintes digitales laissent des traces à chacun de nos gestes les plus quotidiens et peuvent être exploitées à des fins d'identification et de recherche des personnes. Dès lors, une base de données d'empreintes digitales, quelle que soit la finalité initiale de sa constitution, est susceptible d'être utilisée à des fins de police[15].

[15] Rappelons que la police judiciaire est « tiers autorisé » à accéder à tous les fichiers ou traitements pouvant intéresser l'enquête, non seulement lorsqu'une information judiciaire est ouverte et que le juge d'instruction a délivré aux policiers enquêteurs une commission rogatoire leur délégant, en termes parfois très généraux, ses pouvoirs d'investigation, mais aussi lors des enquêtes dites « de flagrance » où les policiers agissent seuls, sous la seule réserve d'un contact téléphonique avec les magistrats du Parquet, et peuvent, sans mandat formalisé, faire toute perquisition en tout lieu, sans qu'à ce stade aucun contrôle juridictionnel sur l'opportunité ou la nécessité de telles investigations ne soit exercé par une juridiction.

Délibération n° 00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Jean Rostand de Nice, destiné à gérer l'accès à la cantine scolaire par la reconnaissance des empreintes digitales

La Commission nationale de l'informatique et des libertés ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 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 le projet d'acte réglementaire du principal du collège Jean Rostand de Nice portant création du traitement ;

Après avoir entendu Monsieur Maurice Benassayag, commissaire, en son rapport et Madame Charlotte-Marie PITRAT, commissaire du Gouvernement, en ses observations ;

Considérant que le collège Jean Rostand de Nice a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis concernant la mise en oeuvre d'un traitement automatisé d'informations nominatives destiné à gérer l'accès à la cantine scolaire des élèves et des personnels ainsi que la facturation, qui comporterait une base de données biométriques reposant sur la reconnaissance automatique des empreintes digitales des personnes concernées ;

Considérant que le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations, dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée, par exemple le contrôle d'accès à des locaux sensibles ; que le surcroît de sécurité et les commodités d'usage qui sont attendus du recours aux techniques biométriques ont pour nécessaire contrepartie l'enregistrement dans une base de données informatique des éléments physiques d'identification des personnes — par exemple, empreintes digitales, ligne de contour de la main, l'iris, la voix — qui seront choisis comme éléments de référence ;

Considérant qu'il y a lieu d'apprécier, dans chaque cas, si la constitution d'une telle base de données est adaptée et proportionnée à l'objectif poursuivi en tenant compte, tout à la fois, des caractéristiques de l'élément

d'identification physique retenu et des usages possibles de telles bases de données ;

Considérant que la base de données que le collège Jean Rostand de Nice souhaite mettre en œuvre associerait aux informations administratives et de gestion une représentation codée des empreintes digitales de l'index de chaque main des élèves et des membres du personnel, le traitement ainsi mis en œuvre ayant pour finalité de faciliter l'accès à la cantine scolaire et la gestion des comptes et de la facturation ; qu'il permettrait, en outre, aux dires de l'établissement, d'éviter toute manipulation d'espèces et les difficultés généralement liées à la perte ou à l'oubli des cartes de cantine ; qu'enfin, le déclarant fait valoir que les élèves, les parents d'élèves ainsi que les représentants du personnel ont été informés du projet dont ils ont approuvé, tout à la fois, le principe et les modalités ;

Considérant cependant qu'à la différence d'autres données biométriques, les empreintes digitales laissent des traces qui peuvent être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main ; que la constitution d'une base de données d'empreintes digitales est dès lors susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création ;

Considérant que si la constitution de bases de données biométriques y compris d'empreintes digitales peut être justifiée dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse, sa mise en œuvre dans un collège, à l'égard notamment de mineurs et aux seules fins de contrôler l'accès à la cantine scolaire est excessive au regard de la finalité poursuivie ;

Émet un avis défavorable à la mise en œuvre du traitement.

IV. LA GESTION DES HORAIRES

La CNIL a eu connaissance du fait que la préfecture de l'Hérault avait mis en place un dispositif technique de lecture des empreintes digitales, dans le cadre de la gestion du temps de travail et des horaires variables des agents territoriaux.

Or, la demande d'avis déposée par cette préfecture auprès de la commission en novembre 1999 concernant la gestion du temps de travail (n° 670979) indiquait exclusivement l'utilisation de lecteurs de badges et non le recours au traitement automatisé d'empreintes digitales.

Le préfet a justifié la mise en œuvre de ce système associant le badge d'accès, qui permet l'identification de l'agent territorial, et le lecteur d'empreintes digitales, qui permet l'authentification de l'agent en empêchant la « fraude aux horaires » entre fonctionnaires, en indiquant qu'« il est très immoral de créditer un agent d'un temps de travail qu'il n'aurait pas effectué et ce grâce à un badgeage effectué par une tierce personne ».

Il était précisé que lors du choix de ce système, l'ensemble des représentants du personnel avait été convié à une présentation chez le fournisseur local. Le bulletin

interne de la préfecture en avait fait état et la préfecture avait précisé que, dans son ensemble, le personnel avait souscrit à ce système, car « il est juste et fiable ».

Le fournisseur du lecteur a précisé que le système ne pouvait fonctionner sans un identifiant « préalable ». Cet identifiant peut être un badge, un code confidentiel... L'authentification d'un agent ne peut s'effectuer que si le système présume de son identité. Techniquement, le code confidentiel ou le badge permet de positionner un gabarit qui sera comparé à l'information issue du capteur d'empreintes.

L'exécution de l'algorithme de création du gabarit est irréversible ce qui ne permet pas de revenir à l'image. L'information obtenue, le « gabarit » (1 kilo octet) représente une simplification extrême par rapport à l'image d'une empreinte. C'est ainsi que la détention d'un ou plusieurs gabarits ne permettrait en aucun cas de remonter ou de recréer l'empreinte des personnes concernées. Par ailleurs, il ne serait pas possible d'imprimer les empreintes des agents.

Il s'agissait donc pour la Commission d'apprécier s'il était admissible ou non qu'une administration constitue une base d'empreintes digitales non pas pour mieux contrôler les accès ou sécuriser les locaux mais pour veiller à ce que des fonctionnaires n'échangent pas, malicieusement, leurs badges pour induire leur hiérarchie en erreur sur les horaires de présence effectivement réalisés. En effet, l'utilisation prévue d'un badge suffirait à elle seule à prévenir toute intrusion dans les locaux non accessibles au public. Le déclarant a certes précisé que la préfecture est un bâtiment sensible, toujours soumis au plan Vigipirate, mais précisément la seule utilisation d'un badge d'accès satisfait à l'exigence de sécurité. Une fois les opérations d'identification et d'authentification effectuées, un logiciel gère les horaires pratiqués par les agents et leur temps de travail et c'est surtout là que réside l'intérêt du système.

La Commission a rendu un avis défavorable à la mise en œuvre du traitement en se fondant également sur le défaut de proportionnalité au regard de l'objectif poursuivi. Éviter une éventuelle « fraude aux horaires » qui résulterait de l'utilisation du badge d'un des membres du personnel par un de ses collègues, ne paraît pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels d'une préfecture.

La préfecture de l'Hérault a indiqué avoir renoncé à ce dispositif.

Par ailleurs, une compagnie aérienne a adressé à la Commission une déclaration relative à un traitement dont la finalité principale est la gestion des horaires au moyen d'une pointeuse biométrique procédant à la reconnaissance des empreintes digitales des employés.

Le système, devant être implanté sur le site de l'aéroport de Roissy-Charles-de-Gaulle, consistait en deux pointeuses biométriques (morphotouch), reconnaissant les 150 employés grâce à leurs empreintes digitales et enregistrant les entrées et sorties afin de déterminer le temps de travail effectué. Les temps de travail seraient cumulés à la semaine ou au mois pour fournir le rapport d'activité de chacun des employés. En pratique, il était prévu que les salariés apposent leur doigt sur la pointeuse qui affiche alors un message indiquant leur nom, date et heure d'arrivée en cas d'authentification réussie ou un message indiquant un échec d'identification.

Dans ce dernier cas, le salarié peut essayer avec le deuxième doigt dont le gabarit a été pris et, en cas de nouvel échec, s'adresser à l'administrateur.

La Commission a informé cette société que le recours à la reconnaissance des empreintes digitales des salariés et la constitution d'une base de données d'empreintes digitales ne lui paraissaient pas proportionnés à la finalité de gestion des temps de présence des salariés. Elle lui a rappelé que le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée. Cependant, le surcroît de sécurité et les commodités d'usage qui sont attendus du recours aux techniques biométriques ont, le plus souvent, pour contrepartie l'enregistrement dans une base de données informatique des éléments physiques d'identification des personnes. En outre, à la différence d'autres données biométriques, telles que le contour de la main, l'iris, ou la voix, les empreintes digitales laissant des traces qui peuvent être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main, la constitution d'une base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création.

C'est au regard de l'ensemble de ces considérations que la Commission apprécie, dans chaque cas, si le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données à caractère personnel sont, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données ainsi constituées, adaptés et proportionnés à la finalité assignée au dispositif.

La Commission a fait valoir auprès de cette société que la constitution d'une base de données d'empreintes digitales aux fins de contrôle de gestion des temps de présence effectués par les salariés lui paraissait excessive et disproportionnée et que, compte tenu de l'intérêt qu'elle portait à cette question et de son rôle d'information général, elle souhaitait que sa position soit transmise au comité d'entreprise de cette société et soit rendue publique au même titre que les avis prononcés le même jour sur des applications similaires.

La compagnie aérienne a décidé de ne pas poursuivre la mise en place de ce système biométrique.

Délibération n° 00-057 du 16 novembre 2000 portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet d'arrêté présenté par le préfet de l'Hérault ;

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

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

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

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

Après avoir entendu Monsieur Hubert Bouchet, commissaire, en son rapport et Madame Charlotte-Marie PITRAT, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

La préfecture de l'Hérault a saisi la Commission d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à permettre l'authentification des agents territoriaux de la préfecture dans le cadre de la gestion du temps de travail et l'établissement d'horaires variables au moyen d'un dispositif biométrique reposant sur la reconnaissance des empreintes digitales des personnes concernées.

La préfecture fait valoir que le badge d'accès, dont l'utilisation permet de conserver trace des heures d'entrées et de sorties du personnel afin de calculer le temps de travail des agents territoriaux soumis à des horaires variables, ne doit pas pouvoir être utilisé frauduleusement par un agent territorial souhaitant dissimuler l'absence ou le retard d'un de ses collègues. C'est la raison pour laquelle la préfecture souhaite, grâce à un dispositif de reconnaissance des empreintes digitales associé à l'utilisation des badges d'accès, éviter toute utilisation d'un badge par une personne autre que son titulaire.

En pratique, chaque agent devrait présenter son badge d'accès à un lecteur de badges qui permettrait de l'identifier puis devrait présenter un de ses doigts devant un lecteur d'empreintes digitales afin que les gestionnaires du personnel soient assurés que la personne ayant présenté le badge en était bien le titulaire et puissent, en conséquence, calculer son temps de présence au travail.

Le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée. Cependant le surcroît de sécurité et les commodités d'usage qui sont attendues du recours aux techniques biométriques ont, le plus souvent, pour contrepartie l'enregistrement dans une base de données informatique des éléments physique d'identification des personnes. Les empreintes digitales font de surcroît partie des données biométriques qui laissent des traces pouvant être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main et dès lors, la constitution d'une base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création.

C'est au regard de l'ensemble de ces considérations qu'il y a lieu pour la Commission d'apprécier, dans chaque cas, si le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données à caractère personnel comportant une telle identification biomé-

trique sont, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données ainsi constituées, adaptés et proportionnés à la finalité assignée au dispositif.

Dans le cas d'espèce, la mise en place d'un badge d'accès étant de nature à prévenir toute intrusion d'un tiers qui n'en serait pas doté dans les locaux de la préfecture, le recours à la reconnaissance biométrique des empreintes digitales des fonctionnaires et des personnels de la préfecture, aurait pour objet d'éviter une éventuelle « fraude aux horaires » qui résulterait de l'utilisation du badge d'un des membres du personnel par un de ses collègues. Un tel objectif ne paraît pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels d'une préfecture. Aussi, le traitement pris dans son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi.

Au bénéfice de ces observations, la Commission **émet un avis défavorable** au projet d'arrêté présenté par le préfet de l'Hérault.

V. LA PROTECTION DE LOCAUX SENSIBLES

La Commission a examiné une déclaration de l'établissement de la Hague de la Cogema (Compagnie générale des matières nucléaires) qui a modifié son traitement de gestion des accès physiques du personnel et des visiteurs, en mettant en place un dispositif de lecteurs d'empreintes digitales pour les salariés et les visiteurs habilités (prestataires de service).

L'objectif est bien évidemment d'assurer la sécurité de l'accès aux différentes zones du site dont certaines sont sous secret défense. Les personnels concernés disposent également de badges permettant de gérer les présences, notamment celles du personnel d'astreinte en interface avec l'application de gestion des ressources humaines. Le système d'identification par empreinte est cependant totalement déconnecté du traitement de gestion des temps de présence.

Les dates et heures d'entrée et de sortie sur le site sont enregistrées et conservées un an pour les salariés et deux ans après la visite pour les visiteurs, « compte tenu de la sensibilité extrême du site, du fait de son activité ». Un récépissé a été délivré.

Le recteur de l'académie de Lille a également transmis à la CNIL une demande d'avis dont la finalité est l'habilitation d'accès pour les personnels de l'Education nationale aux bâtiments de la cité académique par le biais d'un système de contrôle d'accès biométrique par reconnaissance des empreintes digitales. Ce sont environ 1200 personnes qui sont concernées par ce système dont les objectifs sont triples :
permettre un accès rapide et sans contrainte liée à la manipulation de cartes ou badges devant être présentés par les personnels habilités ;
assurer la sécurité des locaux et des personnels dans les bureaux de la direction du recteur (bureau du secrétaire général, du cabinet), les locaux informatiques et cer-

tains locaux à risque tels les archives (dossiers des personnels), imprimerie spécifique pour les sujets d'examens et de concours, salles fortes... — améliorer l'accueil par des hôtesses qui seront plus disponibles pour les publics ou les usagers non habilités.

Il n'est procédé à aucun enregistrement des données relatives aux dates et heures d'entrée des personnels et donc à aucun contrôle du temps de présence. Les sorties sont libres et non gérées par le système. Le recours à la reconnaissance par empreintes digitales est donc exclusivement destiné à s'assurer que seules les personnes habilitées pénètrent dans les locaux du rectorat.

Les représentants du personnel ont été informés de la mise en place de ce système lors d'une présentation générale du projet et chaque division et service de l'académie a été chargé d'informer l'ensemble de ses personnels. Le secrétaire général de l'académie a précisé que le projet d'utilisation du système biométrique n'avait soulevé aucune réaction de rejet de la part du personnel.

La Commission a considéré que le recours à la reconnaissance des empreintes digitales des personnels de la cité académique étant principalement destiné à assurer la fluidité de l'entrée des personnels, les visiteurs extérieurs n'étant pas soumis à un tel système, et à contrôler que seuls les personnels habilités ont accès à tel ou tel local, une telle finalité ne paraissait pas justifier dans sa généralité, la constitution d'une base de données d'empreintes digitales de l'ensemble du personnel de la cité académique ni le recours à un procédé de reconnaissance par éléments d'identification biométrique pour contrôler l'habilitation des personnels à avoir ou non accès à l'ensemble des locaux. En revanche, certains impératifs spécifiques de sécurité, tels que la confidentialité des examens et concours, justifiaient le recours à un tel système dès lors qu'il serait limité à certains locaux déterminés et adapté à la nécessité d'authentifier ceux des membres du personnel habilités à y accéder. L'analyse du dossier a permis de considérer que tel était le cas pour l'imprimerie des sujets d'examen et concours, les salles fortes, les coffres et les salles d'archives contenant notamment les dossiers des personnels. La commission a ainsi limité à ces locaux et aux seuls membres du personnel habilités à y accéder le système de reconnaissance des empreintes digitales et la base de données subséquente et a vérifié les mesures prises afin d'assurer la confidentialité des données.

C'est ainsi qu'elle a relevé que la base de données serait composée de trois modules distincts : le module « personne » qui comporterait les noms, prénoms et identifiants permettant d'accéder aux données d'un autre module ; le module « droit d'accès » qui contiendrait les profils d'habilitation des personnes. Le module « empreintes » qui comporterait les gabarits des empreintes digitales et ferait l'objet d'un cryptage spécifique. Ce module comporterait l'identifiant interne permettant de faire le lien entre le module droits d'accès et les gabarits des empreintes.

Le déclarant a fait valoir que le dispositif de sécurité mis en place ne permettrait pas de procéder à l'impression des gabarits enregistrés et que l'administrateur de la base de la cité académique ne disposerait pas des clés de cryptage et de décryptage qui seraient gardées par le concepteur du produit.

Ces mesures sont apparues satisfaisantes au regard des exigences de confidentialité et de sécurité qu'appelle la constitution d'une base de données de cette nature.

Au début de l'année 2001, le musée du Louvre a déposé un dossier de demande d'avis ayant pour finalité tout à la fois d'assurer la sécurité des biens du musée et de contrôler les heures de travail de certains salariés des entreprises sous-traitantes chargées d'en assurer le nettoyage et la maintenance. Le dispositif biométrique choisi a consisté en celui de reconnaissance du contour de la main.

Le musée du Louvre sous-traite en effet un certain nombre d'activités à des entreprises extérieures : les contrats de sous-traitance prévoient un certain nombre d'heures travaillées qui constituent la base d'évaluation du forfait du marché et le musée veut contrôler la réalité des heures travaillées. La finalité initiale de ce dispositif consiste donc dans un contrôle global des heures par entreprises.

Par ailleurs, compte tenu de la présence des œuvres d'arts, chacun des agents des entreprises sous-traitante doit être agréé, et le musée du Louvre demande lors de l'agrément le bulletin n° 2 du casier judiciaire. L'utilisation de la technique biométrique permet donc aussi de s'assurer que seuls les salariés agréés pénétreront dans le musée pour l'exécution du marché.

L'outil est composé de plusieurs bornes associées à un ordinateur qui stocke les informations par le biais d'une interface spécifique. Lorsque l'image de la main d'une personne doit être enregistrée dans le dispositif, trois mesures sont effectuées de façon à obtenir la forme de la main en trois dimensions. Le système est paramétrable de façon à autoriser un niveau de rejet général plus ou moins élevé selon la sécurité nécessaire.

Le dispositif qui est prévu pour déclencher des ouvertures de porte comporte de façon optionnelle un ordinateur qui enregistre les transactions : heures de passage associées au code de la personne, ainsi qu'une gestion des alarmes et des refus de passage.

Les informations relatives à l'identité de la personne sont conservées par le Louvre tant que le salarié fait partie de l'entreprise prestataire de service et les données relatives aux heures de passage sont conservées pendant un an sur support numérique. La durée de conservation est justifiée par l'obligation incombant aux entreprises de conserver à la disposition des inspecteurs du travail les éléments constitutifs du temps de travail des salariés pendant une année.

La Commission a donné un avis favorable au traitement pour une durée d'un an. Les salariés de toutes les entreprises concernées ont été informés par note de service de l'existence de leur droit d'accès aux données les concernant et de leur droit de rectification de ces mêmes informations.

Dès lors, les informations et leur durée de conservation apparaissent pertinentes et non excessives au regard de la finalité du traitement, dans la mesure où l'élément d'identification physique retenu, consistant en des mesures de la main, est difficilement susceptible d'être utilisé à des fins étrangères à la finalité recherchée par le responsable du traitement. En effet, le contour de la main ne fait pas partie des

données biométriques qui laissent des traces, telles les empreintes digitales, pouvant être exploitées à des fins d'identification.

Le recours à la technique de reconnaissance du contour de la main permet de s'assurer que les données nécessaires au contrôle de l'accès ne sont ni perdues, ni falsifiées, ni échangées, que seules les personnes habilités peuvent pénétrer dans les locaux protégés et présente ainsi un degré de fiabilité. Le traitement apparaît dès lors adapté et proportionné aux objectifs poursuivis par le musée du Louvre.

Toutefois, la Commission a précisé qu'elle souhaitait obtenir un bilan de l'utilisation de cette technique biométrique après 12 mois d'utilisation et qu'elle ne se prononcerait à titre définitif sur le projet de décision qu'à la lumière de ce bilan.

Elle souhaite en effet avoir une vision élargie des dispositifs biométriques existants et de leurs implications en termes de protection de la vie privée et des libertés. Elle a donc décidé d'entreprendre une étude de fond sur tous les dispositifs utilisant des technologies biométriques afin de pouvoir se prononcer en parfaite connaissance de cause dans un an.

Délibération n° 00-056 du 16 novembre 2000 portant avis sur un projet d'arrêté présenté par le ministre de l'Éducation nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès, par la reconnaissance des empreintes digitales de certains personnels de l'Éducation nationale, pour certains locaux de la cité académique de Lille

La Commission nationale de l'informatique et des libertés ; Saisie pour avis du projet d'arrêté présenté par le recteur de l'académie de Lille Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

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

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

Après avoir entendu Monsieur Hubert Bouchet, commissaire, en son rapport et Madame Charlotte-Marie PITRAT, Commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre de l'Education nationale a saisi la Commission d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à contrôler les conditions d'accès des personnels de l'Education nationale aux bâtiments, au moyen d'un dispositif biomé-

trique reposant sur la reconnaissance des empreintes digitales des personnes concernées.

La finalité du traitement est présentée par le déclarant comme étant destinée à assurer la sécurité des locaux tout en facilitant l'accès des personnels ainsi dispensés d'avoir à présenter une carte ou un badge d'accès. Il est précisé que les dates et heures de passage des personnels habilités ne seraient pas enregistrées, le système n'étant pas destiné à vérifier les horaires de présence.

Le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'authentification ou l'identification des personnes doit être parfaitement assurée. Cependant le surcroît de sécurité et les commodités d'usage qui sont attendues du recours aux techniques biométriques ont, le plus souvent, pour contrepartie l'enregistrement dans une base de données informatique des éléments physique d'identification des personnes. Les empreintes digitales font de surcroît partie des données biométriques qui laissent des traces pouvant être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main et dès lors, la constitution d'une base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création.

C'est au regard de l'ensemble de ces considérations qu'il y a lieu pour la Commission d'apprécier, dans chaque cas, si le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données à caractère personnel sont, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données ainsi constituées, adaptés et proportionnés à la Finalité assignée au dispositif.

Dans le cas d'espèce, le recours à la reconnaissance des empreintes digitales des personnels de la cité académique est principalement destiné à assurer la fluidité de l'entrée des personnels, les visiteurs extérieurs n'étant pas soumis à un tel système, et à contrôler que seuls les personnels habilités ont accès à tel ou tel lieu de la cité académique.

Dans sa généralité, une telle finalité ne paraît pas justifier la constitution d'une base de données d'empreintes digitales de l'ensemble du personnel de la cité académique ni le recours à un procédé de reconnaissance par éléments d'identification biométrique pour contrôler l'habilitation des personnels à avoir ou non accès à l'ensemble des locaux. En revanche, certains impératifs spécifiques de sécurité, tels que la confidentialité des examens et concours, sont de nature à justifier le recours à un tel système dès lors qu'il serait limité à certains locaux déterminés et adapté à la nécessité d'authentifier ceux des membres du personnel habilités à y accéder. Il résulte du dossier de demande d'avis que tel est le cas pour les locaux suivants : l'imprimerie (sujets d'examen et concours), les salles fortes, les coffres et les salles d'archives (dossiers des personnels,...).

Ainsi limité à ces locaux et aux seuls membres du personnel habilités à y accéder, le système de reconnaissance des empreintes digitales et la base de données subséquente doivent être entourés de toutes mesures permettant d'assurer la confidentialité des données.

Sur ce point, la Commission relève que la base de données serait composée de trois modules distincts : le module « personne » qui comporterait les

noms, prénoms et identifiants permettant d'accéder aux données d'un autre module ; le module « droit d'accès » qui contiendrait les profils d'habilitation des personnes. Le module « empreintes » qui comporterait les gabarits des empreintes digitales et ferait l'objet d'un cryptage spécifique. Ce module comporterait l'identifiant interne permettant de faire le lien entre le module droits d'accès et les gabarits des empreintes.

Le déclarant fait valoir en outre, d'une part que le dispositif de sécurité mis en place ne permettrait pas de procéder à l'impression des gabarits enregistrés, d'autre part l'administrateur de la base de la cité académique ne disposerait pas des clés de cryptage et de décryptage qui seraient gardées par le concepteur du produit.

Ces mesures satisfont, dans le cas d'espèce, aux exigences de confidentialité et de sécurité qu'appelle la constitution d'une base de données de cette nature.

Au bénéfice de ces observations, la Commission **émet un avis favorable** au projet d'arrêté présenté par le ministre de l'Éducation nationale sous réserve que l'article premier soit ainsi rédigé :

« Il est créé un traitement automatisé d'informations nominatives ayant pour objet le contrôle d'accès, par la reconnaissance des empreintes digitales de certains personnels spécialement habilités, pour les locaux exigeant une confidentialité totale qui sont l'imprimerie spécifique [sujets d'examen et concours), les salles fortes, les coffres et les salles d'archives (dossiers des personnels, etc.). »

Chapitre 5

LA CYBERSURVEILLANCE DES SALARIÉS

La CNIL a entrepris une étude d'ensemble des questions liées au contrôle de l'activité des salariés, en particulier s'agissant de l'utilisation des NTIC, dans le souci de suggérer aux entreprises et aux salariés utilisateurs l'adoption d'une règle du jeu équilibrée, comme les autorités de protection des données l'ont fait lors de l'apparition des précédentes technologies : badges, autocommutateurs, vidéosurveillance, etc.

Le projet de la Commission était d'abord une méthode : consultation d'experts informatiques et tout particulièrement d'experts en réseau, consultation des syndicats de salariés, contact avec celles des entreprises qui ont déjà élaboré des chartes d'usage des intranets.

La CNIL a ainsi rencontré le chargé de la sécurité informatique des Aéroports de Paris, le responsable de la sécurité informatique de Thomson Multimédia, le délégué à la sécurité des systèmes d'information du CNES (Centre national d'études spatiales). Elle a participé aux groupes de travail d'entreprises mettant en œuvre ces technologies, comme Thalès ou EADS, et a consulté les organisations syndicales des salariés (CGT, CFDT, FO, CFTC et CGC) et patronales (MEDEF et CGPME). Elle a eu également à connaître une cinquantaine de chartes « informatiques et libertés » adoptées par les entreprises qui ont sollicité son avis ou son conseil.

C'est également sur la base des déclarations reçues à la Commission, des chartes élaborées dans les entreprises et de cette large concertation que la CNIL a rendu public le 28 mars 2001 un rapport relatif à la cybersurveillance des salariés dans l'entreprise, autour duquel elle souhaite que s'engage un débat entre entreprises et salariés, responsables informatiques et juristes, instances représentatives et organisations professionnelles.

Ce rapport s'articule autour de grands constats. Des constats techniques : d'une part, l'inhérent traçage lié à l'informatique et, d'autre part, l'existence d'outils destinés à assurer la sécurité des réseaux qui permettent également par un effet secondaire de contrôler l'activité des salariés. Des constats juridiques ensuite, sur les textes législatifs applicables et surtout sur la jurisprudence intervenue en la matière.

I. LES CONSTATS TECHNIQUES

Certaines applications ont, par nature, vocation à fournir à l'entreprise, par traçage informatique, le moyen de prouver la réception des ordres envoyés par la clientèle, l'accomplissement d'une prestation ou l'exécution d'une procédure.

Dans de nombreux cas, l'application informatique n'est qu'un système de traçage à l'état pur, se surajoutant en quelque sorte à une opération manuelle ou intellectuelle. Le traçage informatique vient en renfort dans le seul but de noter tous les gestes exécutés, les décisions prises, afin de permettre la vérification ou d'apporter la preuve que tout a été exécuté selon les règles : le contrôle aérien, les manœuvres sensibles dans les centrales nucléaires, le suivi d'une chaîne de production dans un atelier...

Ce traçage constitue une des meilleures mesures de sécurité des fichiers informatiques, sous l'appellation de système de « journalisation ». Qui a consulté quoi ? ◦ quel moment ? Qui a procédé à la modification de telle information enregistrée dans un fichier ?

A. Les outils techniques de surveillance du réseau

Toute informatique d'entreprise ou d'administration comporte une fonction de *gestionnaire de réseau.* Ce métier consiste à installer ou à maintenir les éléments actifs énumérés ci-dessus, à installer les logiciels réseau sur les ordinateurs centraux et les postes de travail, à les mettre à niveau quand de nouvelles versions sont mises sur le marché par les fournisseurs, etc. Mais l'une des activités principales du gestionnaire de réseau réside dans la surveillance du réseau, pour détecter les pannes, déceler les engorgements, mieux répartir les charges. Ce contrôle peut être permanent ou réalisé « par campagne ». Les outils de surveillance mis à la disposition de l'administrateur réseau vont du plus frustre à des systèmes très sophistiqués.

Le premier type de traçage se situe au niveau de la *couche logicielle* la plus primitive, la couche dite « basse » : tout ce qui sort ou entre dans l'ordinateur par la voie du réseau, le moindre bit, est mémorisé dans un fichier de traces. L'objectif de ce traçage est de permettre aux informaticiens de rechercher les causes de « bogues » de logiciel ou de mauvaises performances du système.

Le niveau suivant est celui du *moniteur transactionnel* qui connaît la notion de transaction, c'est-à-dire des séquences plus élaborées que les simples séquences de bits et ayant un sens sémantique plus riche. Il génère ses propres fichiers de

traces. La lecture d'un fichier de traces d'un moniteur transactionnel est de ce fait plus facilement exploitable et instructive : on pourrait y lire, sans grande peine, qui a fait quoi et à quelle heure.

Le dernier niveau de traçage est celui fourni par *l'application (traces ou logs).* Dans la plupart des cas, les informaticiens développeurs y ont ajouté une fonctionnalité qui permet de tracer de façon synthétique, presque en clair, l'activité des utilisateurs.

En résumé, certains produits permettent, d'origine ou selon le paramétrage effectué, seulement de mesurer des débits. D'autres vont permettre la surveillance simultanée de plusieurs routeurs. D'autres encore permettront, par exemple, de mesurer le nombre d'appels, les durées des consommations et les seuils d'alerte. Cela signifie qu'il est possible de savoir qui s'est connecté, à quel site, à quelle heure et pendant quelle durée, quelles sont les tentatives de connexion qui ont échoué, etc.

LES PARE-FEU OU « FIREWALL »

Tout serveur accessible à partir d'Internet, soit directement soit indirectement par rebond, doit se protéger des attaques extérieures. Un pare-feu est un produit logiciel ou matériel assurant au minimum la protection d'un réseau interne d'attaques externes. Il permet également la protection des réseaux internes les uns par rapport aux autres, le filtrage des communications, l'authentification, le cryptage et le contrôle des accès utilisateurs par rapport aux réseaux.

Le pare-feu est, de par sa nature, le meilleur gardien de l'entreprise puisque, bien paramétré, il protège efficacement l'entreprise des agressions extérieures et évite les connexions considérées comme inappropriées par l'entreprise. Mais il peut aussi devenir le meilleur « espion » de l'activité Internet : rien ne peut se faire sans qu'il le ne le sache, jusqu'au plus petit détail. Il détiendra de ce fait toutes les traces de l'activité qui transite par lui : détails de la navigation sur Internet (sites visités, heures des visites, etc.), les détails de messages envoyés et reçus : expéditeur, destinataire (s), objet, nature de la pièce jointe, et éventuellement texte du message.

LES PROXYS

La fonction d'un serveur proxy est de mémoriser les pages web consultées par les internautes de sorte qu'en cas de nouvelles requêtes vers ces sites ou les pages des sites précédemment consultés, il ne soit pas nécessaire d'accéder au serveur distant, ce qui économise ainsi de la bande passante et permet une connexion beaucoup plus rapide. Pour ce faire, chaque demande de consultation d'une page web sera précédée d'une requête vers le serveur proxy afin de savoir s'il ne détient pas une copie de la page ou si la page n'a pas été modifiée entre-temps. Toutefois, un serveur proxy ne dispose pas d'un espace disque illimité : il lui faut constamment libérer de la place pour mémoriser de nouvelles pages en éliminant les pages les plus anciennes ou les moins référencées.

L'entreprise pourrait profiter de la fonction de mémorisation du serveur proxy pour surveiller l'utilisation d'Internet par ses salariés puisqu'un serveur proxy connaît nécessairement l'adresse IP de l'internaute à qui il doit renvoyer une page web. Toutefois ce constat mérite d'être relativisé dans la mesure où la plupart des serveurs proxy sont hébergés hors de l'entreprise, chez le fournisseur d'accès par exemple, et ne sont donc pas « sous les yeux » de l'employeur.

Enfin, il convient de préciser que tout internaute a le choix de renoncer à l'usage du proxy, mais au prix d'une baisse des performances, en « décochant » l'option proxy dans son navigateur.

LA MESSAGERIE

La messagerie occupe une place de choix dans le monde de l'Internet en permettant à deux internautes de communiquer à travers l'envoi et la réception de messages écrits identifiés par une adresse « e-mail ».

La différence fondamentale entre un appel téléphonique et un message électronique consiste dans la volatilité du premier et la pérennité du second. En effet, l'appel téléphonique s'achève aussitôt le combiné raccroché. Le message électronique, lui, demeure sur le disque dur de l'utilisateur et trace en est conservée sur le serveur de messagerie et au niveau du pare-feu.

De surcroît, des programmes peuvent également être écrits, sans difficultés particulières, pour « traiter » à des fins de surveillance et selon des critères tels que des mots clefs, la référence du destinataire, la présence et/ou le volume du fichier joint, le format (texte, image), le contenu des messages.

LE DISQUE DUR DE L'UTILISATEUR

L'ordinateur de l'internaute conserve dans sa « mémoire cache » les pages qui ont été visualisées, dans le but de pouvoir les afficher plus rapidement et facilement si elles sont demandées de nouveau. L'ordinateur enregistre également les informations qui lui sont envoyées par les sites : les cookies ou les applets.

L'utilisation de la **mémoire cache** est un moyen d'optimiser les temps de chargement et de désengorger le réseau. Son principe est analogue à celui du proxy évoqué ci-dessus : éviter de solliciter inutilement les serveurs distants de sites web quand l'internaute consulte fréquemment les mêmes pages. Mais, à la différence du proxy qui est sur un serveur externe, ici les pages sont mémorisées sur le micro de l'internaute au fur et à mesure de leur consultation. Si cette fonctionnalité est présente sur le navigateur, lorsque une requête est lancée, le navigateur commence par aller voir sur un répertoire du disque dur si la page HTML demandée n'aurait pas été chargée auparavant. Si tel n'est pas le cas, il effectuera alors la requête auprès du proxy, puis auprès du serveur distant, mais lorsque son résultat arrive, il sera enregistré sur le disque en même temps que présenté à l'écran. La fois suivante, si la même requête est lancée, le navigateur ira simplement lire la page sur le disque.

Un **cookie** est un enregistrement d'informations par le serveur dans un fichier texte situé sur l'ordinateur client, informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement. La technique des cookies repose sur le protocole HTTP, qui est le langage de communication du web. Il ne faut donc pas voir des cookies partout : seul un serveur web peut en envoyer et aller les relire pour exploiter leur contenu.

Le logiciel de **messagerie** installé sur un ordinateur stocke tous les messages envoyés et reçus par cet ordinateur. La suppression d'un message sur un ordinateur demande deux opérations : sa suppression dans la boîte à lettres active, de « réception » pour un message reçu ou « d'envoi » pour un message envoyé, puis la suppression du fichier dit « poubelle » dans lequel il a été stocké après la première opération. Mais de telles opérations sont vaines, du point de vue de la discrétion, si une sauvegarde des données existe par ailleurs. Aussi est-il essentiel que tout salarié soit informé de l'existence d'une sauvegarde et de la durée pendant laquelle les données sont conservées.

Enfin, la configuration basique de l'ordinateur, sa nature même, permet de retrouver tout ce qui a été fait sur cette machine. Cette mémoire permet de retrouver toute l'information traitée sur cet ordinateur, y compris en cas de suppression ou en cas de perte dû à un arrêt brutal du travail en cours. Tel est l'avantage. Le revers de cette fonction de base est qu'elle permet, sans utiliser les technologies déjà détaillées, de retrouver disséminés dans le disque dur : l'heure de la dernière modification d'un fichier quel qu'il soit (y compris ceux que le salarié aurait enregistrés dans son répertoire dit « personnel »), les pages web vues, les messages envoyés et reçus.

Les traces peuvent être classées en trois catégories : pour les besoins de l'entretien du système à titre préventif ou curatif : détecter les pannes, améliorer les performances ; pour les besoins de sécurité, en n'autorisant l'accès au système qu'aux seuls utilisateurs habilités et savoir qui fait quoi ; pour restreindre, par filtrage, certaines actions des utilisateurs (censure) considérées par les entreprises comme étant hors du champ de leurs activités.

L'informatique ne peut fonctionner sans trace, sinon l'informaticien aurait à gérer le système en aveugle, les événements survenant dans un ordinateur étant trop nombreux et se déroulant trop vite. En outre, en informatique, toute activité d'un utilisateur est « traçable »... y compris sa non activité.

B. La vie privée du salarié a émergé dans l'entreprise par les lois « Auroux »

En précisant que le règlement intérieur ne pouvait apporter aux droits et libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nécessité de la tâche à accomplir ni proportionnées au but recherché, l'article L 122-35 du code du travail, dans sa rédaction issue de la loi de 1982, a donné, selon le professeur Gérard Lyon-Caen, un « coup de clairon » qui a « ouvert les oreilles » et permis à la jurisprudence de livrer ses premiers arbitrages.

Mais encore, la loi du 4 août 1982 ne posait-elle de limites tenant à la proportionnalité des moyens employés au regard des fins poursuivies qu'au seul règlement intérieur, laissant hors de portée les stipulations du contrat de travail lui-même et les documents qui lui sont annexés, lesquels peuvent contenir d'importantes restrictions aux libertés personnelles.

La loi du 31 décembre 1992, très largement inspirée des propositions du rapport Lyon-Caen et de la doctrine dégagée par la CNIL en matière de traitements automatisés d'informations nominatives, viendra compléter et renforcer ce dispositif.

Ainsi, l'interdiction d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché, n'est plus cantonnée par l'article L 120-2 du code du travail au seul règlement intérieur et s'impose à tous. Parallèlement, l'article L 122-39 soumet au même régime juridique que le règlement intérieur lui-même toutes les notes de service ou tout autre document qui portent prescriptions générales et permanentes dans les matières qui relèvent du règlement intérieur, c'est-à-dire notamment les conditions d'utilisation des équipements de travail et les règles générales et permanentes relatives à la discipline.

Il en résulte que de telles notes de service ou documents portant prescriptions générales doivent désormais être soumis à l'avis du comité d'entreprise ou, à défaut, à l'avis des délégués du personnel (article L 122-36) et que l'inspecteur du travail peut à tout moment exiger le retrait ou les modifications des dispositions qui seraient considérées comme portant une atteinte disproportionnée aux droits des salariés (article L 122-37).

Dans le même esprit, la loi du 31 décembre 1992 fait obligation à l'employeur d'informer et de consulter le comité d'entreprise, préalablement à la décision de mise en œuvre de moyens ou de techniques permettant un contrôle de l'activité des salariés (article L 432-2-1), et, prolongeant les principes de la loi « informatique et libertés » dans le code du travail, précise qu'« 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 ».

Ainsi, trois limites se trouvent imposées au pouvoir de direction de l'entreprise en matière de contrôle et de surveillance des salariés : la transparence, la proportionnalité et la discussion collective.

L'obligation de transparence inspirait déjà 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.

La transparence, entendue comme l'information préalable et la loyauté, est donc une condition nécessaire. Elle n'est pas suffisante. Sans doute plus subjectif et plus délicat de mise en œuvre, le principe de proportionnalité ne s'en impose pas

moins comme une condition indispensable à la régularité d'un système de contrôle et de surveillance d'un salarié sur son lieu de travail. Mais proportionné par rapport à quoi ?

La valeur protégée est, selon les textes considérés, la « vie privée » ou les « droits des personnes et libertés individuelles » invoqués par l'article L 120-2 du code du travail ou encore « l'identité humaine, les libertés individuelles ou publiques » au sens de l'article premier de la loi du 6 janvier 1978. Mais il ne s'agit ici que de textes nationaux. Ils ne sont, cependant, pas seuls en cause.

La discussion collective est organisée par le code du travail lors de l'introduction dans l'entreprise de traitements automatisés de gestion du personnel ou de moyens et techniques permettant un contrôle d'activité du salarié (article L 432-2-1 du code du travail) : elle donne sa substance au principe de proportionnalité. Le rapport inégal entre l'employeur et ses salariés, consubstantiel à la nature même du contrat de travail et au lien de subordination qui le caractérise, ne garantit pas naturellement la proportionnalité.

C. Des principes consacrés au plan européen et mondial

Ces principes ont été consacrés au plan européen et mondial par la Recommandation n° R (89) du comité des ministres du Conseil de l'Europe aux États-membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, du 18 janvier 1989 et par le Recueil de directives pratiques sur la protection des données personnelles des travailleurs adopté par le Bureau international du travail le 7 octobre 1996.

Ce recueil de directives pratiques prévoit qu'une surveillance électronique peut être mise en oeuvre à certaines conditions : d'une part, les données recueillies à cette occasion ne doivent pas être l'unique source de l'évaluation du salarié ; d'autre part, dans les cas où une surveillance est mise en œuvre, les salariés doivent avoir été informés à l'avance des motivations de cette surveillance, des périodes concernées, des techniques utilisées ainsi que des données collectées.

Il est ainsi indiqué qu'une surveillance permanente ne saurait être autorisée que pour des raisons de santé et de sécurité et en vue de protéger les biens de l'entreprise.

II. UN CONSTAT JURISPRUDENTIEL

Ce rapport d'étude fait également le point sur les nombreuses décisions de jurisprudence intéressant directement ou indirectement la matière. Ces décisions relèvent, le plus souvent, du contentieux disciplinaire et du licenciement dans le cadre du contrat de travail et non directement de la vie privée. Cependant, qu'il s'agisse de l'usage à des fins privées des outils mis à la disposition des salariés sur leur lieu de travail ou des moyens de surveillance et de contrôle utilisés par l'employeur, c'est une

jurisprudence de la « proportionnalité » qui s'esquisse, dessinant les contours du respect de la vie privée des salariés par leur employeur.

La plupart des commentaires que les décisions ont suscités s'attachent cependant principalement au contentieux de la preuve, sans s'attarder sur le fond du droit, pourtant essentiel : que reste-t-il de la vie privée du salarié sur le lieu de travail, une fois la justice passée ? Les décisions les plus importantes, publiées ces dernières années, ont été explorées dans cette perspective.

LE CONTENTIEUX DE LA PREUVE

Le contentieux de la preuve peut être décliné en quelques principes simples, liés à l'exigence de la qualité de la preuve et de son appréciation : récusation de la preuve rapportée par un dispositif de contrôle mis en place à l'insu du salarié ; récusation de la preuve rapportée par un traitement automatisé d'informations nominatives non déclaré à la CNIL ; récusation de la preuve rapportée par un traitement d'informations nominatives régulièrement déclaré à la CNIL lorsque l'information en cause est sans rapport avec la finalité du traitement.

Une preuve de qualité est également exigée. Celle-ci doit être rapportée par un dispositif présentant des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu. De plus, la preuve ne doit pas pouvoir être manipulée entre la date des faits et celle des débats.

Toutefois, à en rester sur le terrain de la validité de la preuve, on reste sur le terrain de la loyauté. L'article 1134 du code civil précise que les conventions légalement formées tiennent lieu de lois à ceux qui les ont faites et doivent être exécutées de bonne foi. La loyauté est le complément nécessaire du contrat. Elle apporte d'ailleurs au salarié des garanties essentielles. Mais la loyauté n'est pas à sens unique : là où elle interdit à un employeur de procéder clandestinement ou à l'insu du salarié, elle peut priver un cadre pleinement conscient des usages des écoutes téléphoniques, des architectures en réseau ou d'Internet, de l'argument consistant à reconnaître qu'il a failli mais que la preuve rapportée devrait être récusée au motif qu'il n'avait pas formellement été informé d'un système dont il ne pouvait ignorer ni l'existence ni la portée.

On ne saurait en tout état de cause limiter le débat sur la vie privée ou la surveillance dans le milieu du travail à une seule bataille de procédure, quelquefois décisive mais toujours incertaine. Au demeurant, nul n'aurait à y gagner. En tout cas, pas les salariés puisque à ne se situer que sur le terrain de l'information préalable, il suffirait à un employeur d'informer précisément les salariés de ses choix de direction pour priver ces derniers de l'ensemble de leurs droits et libertés. C'est précisément ce que proscrit le principe de proportionnalité auquel les juridictions veillent, notamment dans le cadre du contentieux des sanctions disciplinaires et du licenciement.

LE SECRET DES CORRESPONDANCES

Le contentieux du fond porte sur le secret des correspondances et l'usage à des fins privées d'outils mis à disposition par l'employeur. C'est dans le domaine de la correspondance écrite que la jurisprudence est la plus ancienne. Le secret de la correspondance est une liberté publique et le principe qui domine toute la matière est celui de l'inviolabilité des correspondances.

Rien n'interdit à un employeur de proscrire l'envoi à l'adresse de l'entreprise de courriers destinés personnellement aux salariés. Mais une telle interdiction ne lui permettrait ni d'ouvrir ni de retenir le courrier litigieux si l'enveloppe porte la mention « personnelle » ou « confidentiel ».

La jurisprudence relative à l'utilisation à des fins personnelles de la ligne téléphonique professionnelle est abondante. Dans de nombreuses affaires, l'usage du téléphone à des fins privées a été jugé constitutif d'une faute grave. Dans d'autres espèces cependant, un usage du téléphone à des fins privées, s'il peut constituer une cause réelle et sérieuse de licenciement, n'est pas jugé constitutif d'une faute grave justifiant un licenciement sans préavis.

Ainsi, au travers du contentieux de la régularité du licenciement, la jurisprudence dessine-t-elle les contours d'un usage admissible du téléphone professionnel à des fins privées. Bien naturellement, tout est question de mesure et, au fond, de loyauté dans les relations réciproques entre employeur et salarié. ◦ défaut d'abus manifeste et caractérisé, un employeur ne saurait reprocher un comportement s'il n'a pas préalablement déterminé quelle était la règle. En outre, la jurisprudence, dans sa diversité, paraît exiger en cette matière qu'une mise en garde précède une sanction telle que le licenciement. Enfin, les juges s'attachent à l'ensemble des circonstances concrètes liées aux faits reprochés au salarié, n'hésitant pas à débusquer sous le prétexte d'un usage abusif du téléphone la volonté réelle de l'employeur.

Le recensement des décisions publiées au sujet de l'utilisation du Minitel à des fins privées manifeste encore une assez grande tolérance des juridictions à l'égard de l'usage par les salariés du Minitel à des fins privées.

Certes, plusieurs décisions retiennent la faute grave. Mais les décisions les plus nombreuses exonèrent le salarié de toute faute, généralement au motif que la preuve n'est pas rapportée que le salarié en cause ait été le seul utilisateur possible du Minitel.

Naturellement, les décisions de jurisprudence sont moins nombreuses s'agissant d'Internet et la plupart de celles qui sont connues relèvent, pour l'heure, des seuls conseils de prud'hommes. Il est dès lors difficile d'en tirer un enseignement général, même si les premières décisions connues paraissent témoigner d'une rigueur particulière à l'égard de l'usage à des fins privées de la messagerie électronique ou du web.

S'il ne fait guère de doute qu'un message électronique relève de la loi du 10 juillet 1991, il ne bénéficie pas pour autant d'une garantie d'absolu secret. La loi de 1991 autorise en effet, dans certaines circonstances et à certaines conditions, les interceptions ordonnées par l'autorité judiciaire et les interceptions dites de sécurité ; elle ménage également, hors le cas dans lequel le fait punissable est commis par une

personne dépositaire de l'autorité publique, l'excuse de bonne foi, justification légale de l'interception, qui fait alors tomber l'infraction. Aussi un employeur peut-il, dans les mêmes conditions juridiques, intercepter un message électronique ou faire procéder à une écoute.

En outre, le point de savoir si la lecture d'un message stocké, sur le disque dur de l'ordinateur du salarié ou par un dispositif technique mis en œuvre au niveau du pare-feu s'apparente ou non à une « interception » au sens de la loi de 1991 demeure entier.

En définitive, il résulte des quelques décisions existantes que les messages électroniques échangés par des salariés ne sont pas protégés de manière absolue par le secret des correspondances. Ils ne le sont que de manière relative. Et relative à deux égards :
d'une part, parce que la loi de 1991 ne prive pas un employeur de la possibilité de placer les salariés sous écoute téléphonique, dès lors qu'il peut attester de sa bonne foi,
d'autre part, parce qu'il est trop tôt pour considérer comme incontestablement établi, compte tenu des termes divergents de la jurisprudence à cet égard, que la lec ture d'un mail stocké sur un serveur de messagerie ou sur le disque dur d'un micro or dinateur serait constitutif d'une interception de communication au sens de l'article 226-15 du code pénal.

De surcroît, les premières décisions prud'homales paraissent, en l'état, témoigner d'une sévérité plus grande à l'égard de l'usage à des fins privées des mes-sageries professionnelles qu'à l'égard de moyens plus traditionnels de communication, tels que le téléphone ou le Minitel.

Si elle devait se confirmer, faudrait-il déduire d'une telle tendance jurispru-dentielle que cette sévérité spécifique à l'Internet serait liée à la nouveauté ?

III. UNE CONCLUSION PROVISOIRE

La Commission a conclu de façon provisoire, en attendant les contributions apportées par la consultation publique ouverte sur son site web et les conclusions définitives qui en résulteront, que la sécurité informatique dans l'entreprise est un objectif qui doit être partagé et qui ne peut être atteint que dans un climat de loyauté et de confiance réciproque. Cet objectif ne peut être parfaitement réalisé que si les salariés sont convaincus qu'il n'est en rien contraire à leur intérêt, à leurs droits et à leurs libertés. Ces conclusions sont au nombre de quatre.

La Commission a estimé que c'est autour de la confiance, de la transparence et de la loyauté, érigées en principes fondateurs, que doit se construire la surveillance. L'efficacité est à ce prix pour la meilleure implication des parties prenantes dans l'entreprise qui a le devoir de se protéger. Ses dirigeants doivent exercer le contrôle de l'exécution du contrat de travail. De leur côté, les salariés ont droit au respect de leur vie privée, laquelle ne peut s'arrêter en pratique à la porte de l'entreprise.

La loyauté s'impose en pratique pour établir le point d'équilibre entre droit de l'employeur à connaître ce qui est nécessaire à l'exercice de sa fonction dirigeante et le droit du salarié à protéger sa vie privée dont l'essentiel n'a pas à être exposé dans la relation de travail.

L'établissement du point d'équilibre ne va pas de soi. Il ne peut résulter que d'un compromis dont le débat seul peut poser les conditions. En faire l'économie revient à entraver l'implication des salariés. Cette dernière postule la certitude que la sécurité informatique dans l'entreprise ne soit en rien contraire aux intérêts, aux droits et à la liberté des salariés. L'ignorance des principes ou la précipitation ont guidé la rédaction de chartes éloignées de l'application du principe de confiance.

Ces chartes sont souvent un cumul d'interdictions d'usage et d'avertissements peut-être de nature à entamer la productivité des salariés qui ne peut se développer que dans un climat de confiance. Au demeurant, les premières décisions des juridictions de l'Union européenne évoquent les *« usages généralement et socialement admis* » de la messagerie et du web à des fins privées et paraissent admettre, comme les juridictions françaises l'ont fait pour d'autres outils, tels que le téléphone ou le Minitel de l'entreprise, un usage à des fins privées dans des limites raisonnables.

La sécurité informatique conditionne la pérennité de l'entreprise : il existe toutefois des limites à sa mise en oeuvre. Elle peut faire l'objet d'un plan d'ensemble porté à la connaissance des salariés et de leurs représentants.

Les mesures de sécurité informatiques arrêtées dans le cadre d'un plan d'ensemble et qui permettent de conserver trace des flux d'informations dans l'entreprise doivent être exposées de manière claire et précise aux salariés, à leurs représentants et au comité d'entreprise. Cette information préalable, dont la majorité de la jurisprudence française paraît admettre le caractère obligatoire, soit au titre du principe de loyauté, soit parce qu'il s'agit de traitements automatisés d'informations nominatives, constitue en tout état de cause la meilleure prévention possible des abus.

• Lorsqu'un pare-feu est mis en place, associé ou non à d'autres outils, la signification des informations enregistrées et leur durée de conservation doivent être précisées aux salariés.

• Lorsqu'une copie de sauvegarde des messages est effectuée, la durée pendant laquelle les messages sont conservés doit être précisée.

• L'interdiction faite aux salariés de disposer d'une messagerie sur un ser veur de messagerie gratuite peut constituer une mesure de sécurité légitime pour l'entreprise, compte tenu des risques (contamination de virus, intrusion, etc.).

• De même, l'interdiction faite aux salariés de laisser leur adresse de mail professionnelle dans des forums de discussion peut, dans certains circonstances, être jugée pleinement justifiée et proportionnée à un objectif de sécurité de l'entreprise.

• Les systèmes de journalisation des connexions destinés à sécuriser l'accès à des fichiers informatiques et, tout particulièrement, à ceux qui comportent des don nées à caractère personnel sont non seulement légitimes mais indispensables. Les

salariés doivent être informés de leur existence, ainsi que de leurs conséquences, ce qui constitue là encore la meilleure manière de prévenir tout accès non autorisé.

• Les administrateurs de système habilités à avoir accès aux données de connexion doivent être identifiés. En outre, les salariés de l'entreprise devraient être informés des autorités hiérarchiques habilitées à requérir des administrateurs des mesures de surveillance particulières lorsque des dérives de nature à porter atteinte à l'intérêt des entreprises seraient constatées. Dans une telle hypothèse, les règles de procédure, d'information du personnel ou de leurs représentants devraient être précisées.

Le problème le plus délicat à gérer pour les employeurs est l'utilisation à des fins personnelles des moyens de communication de l'entreprise par ses salariés. Hier le téléphone et le Minitel, aujourd'hui le web et la messagerie focalisent l'attention sur les usages extraprofessionnels des moyens mis à disposition des salariés. La crainte de certains employeurs concerne le risque de détournement par le salarié d'un temps contractuellement dédié au travail. Elle concerne ainsi plus concrètement la crainte de l'attrait de sites particuliers tels les sites pornographiques et les sites de jeux.

S'agissant de l'usage à des fins extraprofessionnelles par les salariés des moyens mis à leur disposition (web, messagerie), il y a lieu d'observer que seule est en cause la crainte de certains employeurs que la diversité de l'offre de contenus sur Internet soit de nature à distraire dans des proportions inacceptables le salarié de sa tâche.

S'il est légitime que les salariés soient soumis à des contrôles de productivité ou de qualité de leur travail, de tels contrôles ne sauraient être abandonnés à une implacable et systématique surveillance électronique.

NAVIGATION SUR LE WEB A TITRE PRIVE

La solution du filtrage de certains sites — bien que n'étant pas parfaitement efficace — paraît préférable à une interdiction absolue et de principe faite aux salariés de naviguer sur le web.

Il devrait être admis, par la plupart des entreprises, que les salariés peuvent se connecter au web au moins hors de leur temps de travail, quitte à ce que soient posées certaines interdictions à l'égard de sites web à caractère particulier (pornographie, négationnisme, jeu, etc.).

Dans une telle hypothèse, le contrôle a *posteriori* de l'usage fait par les salariés d'une telle tolérance peut être légitime. Cependant, un tel contrôle peut être gradué et ne devrait pas, sauf circonstances exceptionnelles, porter sur une analyse individuelle des sites consultés et de leur contenu. Peut être mis en place un contrôle du temps de connexion par poste sans identification des sites consultés ou encore un contrôle des sites les plus souvent consultés depuis l'entreprise sans ventilation par poste. De tels contrôles dépourvus de caractère nominatif devraient dans la plupart des cas s'avérer largement suffisants. Les salariés devraient en tout état de cause en être informés.

UTILISATION A TITRE PERSONNEL DE LA MESSAGERIE

L'interdiction de principe faite aux salariés d'utiliser la messagerie électronique à des fins non professionnelles paraît tout à la fois irréaliste et disproportionnée.

La sécurité de certaines entreprises particulières peut sans doute justifier que soit opéré un contrôle a *posteriori* de l'usage des messageries. Mais un tel contrôle doit pouvoir être effectué à partir d'indications générales de fréquence, de volume, de la taille des messages, du format des pièces jointes, sans qu'il y ait lieu d'exercer un contrôle sur le contenu des messages échangés.

En tout état de cause, s'agissant des messages « entrants » (adressés par une personne extérieure à l'entreprise à un salarié sur son lieu de travail), toute indication portée dans l'objet du message et conférant indubitablement à ce dernier un caractère privé devrait, selon les principes posés par la jurisprudence sur la correspondance postale, interdire à l'employeur d'en prendre connaissance.

Enfin, il est apparu à la Commission que la confiance des salariés dans leur entreprise ainsi que la confiance que l'employeur fait à ses salariés passaient nécessairement par l'information et la négociation.

La sécurité et l'usage des moyens mis à la disposition des salariés par l'entreprise revêt une dimension nouvelle que la société de l'information amplifie. Les risques pour la sécurité sont accrus par l'avènement de l'information comme matière première principale de l'entreprise et du travail. L'information s'enrichit de l'échange d'interlocuteurs qui la captent et l'enregistrent avant de la remettre en circulation sur le réseau. L'entreprise est un réseau d'informations qu'il convient de protéger.

De son côté, au travail, le salarié dispose de droits et de libertés qui peuvent être encadrés ou restreints, mais ne peuvent être supprimés. Toute restriction ou encadrement doit être proportionné et ne saurait être excessif au regard des nécessités de l'activité professionnelle.

Pour ce qui est de l'utilisation non professionnelle et privée des outils mis à disposition du salarié par l'entreprise, la notion d'usage raisonnable a déjà porté ses fruits aux étapes antérieures de la technologie.

Cela conduit la CNIL à recommander une installation des préoccupations liées aux usages de l'informatique au cœur de la négociation entre les employeurs et les salariés aux différents niveaux interprofessionnels de branches et d'entreprises. Le parti pris de la confiance, pour l'efficacité, implique la discussion éclairée.

La discussion doit se dérouler dans les instances qui existent et déboucher sur le compromis entre les parties.

Le document adopté (charte, code de conduite...) prescrirait de façon détaillée les applications diverses avec leur finalité pour satisfaire au principe de proportionnalité. De ce point de vue, l'entreprise n'est pas uniforme et il convient d'approprier la proportionnalité et la finalité à chaque situation particulière. Toutes n'exigent pas le même degré de sécurité et de surveillance.

L'extrême rapidité de l'évolution des techniques et l'adjonction de fonctionnalités nouvelles doivent conduire à ce que tout accord fasse l'objet d'une mise à jour périodique. ◦ cette fin, on pourrait par exemple envisager que le bilan social de l'entreprise comporte un chapitre dédié au traitement des données personnelles et aux outils de surveillance mis en œuvre dans l'entreprise.

Enfin, les incidences d'une surveillance électronique sur la vie du salarié dans l'entreprise, sur l'idée qu'il se fait de la confiance qu'on lui accorde et sur l'estime de soi pourraient conduire à conférer une responsabilité particulière, en ce domaine, au Comité d'hygiène, de sécurité et des conditions de travail (CHSCT) afin que ces questions puissent être évoquées périodiquement.

Chapitre 6

SANTÉ EN LIGNE

I. MON E-DOCTEUR

Qu'il s'agisse d'obtenir des conseils sur les précautions à prendre en cas de varicelle, de participer à un forum de discussion sur la dépression nerveuse ou le viagra, de créer son dossier médical en ligne, les sites web consacrés à la santé se multiplient et offrent une gamme de services de plus en plus étendue (5 000 sites français recensés en avril 2000 pour 15 000 aux Etats Unis).

On est encore loin, en France, de la consultation médicale ou de la prescription en ligne, en bref, du « super médecin référent virtuel », de la « cybermédecine » qui, aux Etats Unis, semble connaître un certain essor.

Mais si les sites français sont, aujourd'hui, essentiellement des sites d'information et de conseil tournés vers les professionnels de santé et le grand public, l'approche américaine fait des émules...

Le développement de l'« e-santé » appelle sans aucun doute une vigilance particulière et il semble dès lors nécessaire de définir des règles de conduite précises tant en ce qui concerne la confidentialité et le respect des droits des internautes que les modalités d'utilisation des données. Dans quelle mesure, en effet, est-il admissible que les données à caractère personnel recueillies sur les sites santé — qu'il s'agisse des questions posées par les internautes, du dossier de santé ou même des données de connexion — soient utilisées pour cibler les « profils de santé » des internautes et faire ainsi l'objet d'exploitations commerciales ?

Au titre de sa mission de conseil, la CNIL a ainsi décidé de mener une étude d'ensemble des sites santé en France :

A cet effet, deux actions complémentaires ont été engagées :

— la réalisation, auprès de 6 sites, de missions de contrôles sur place, afin d'une part de vérifier les modalités d'exploitation des données collectées et d'autre part d'avoir une meilleure compréhension du fonctionnement et des stratégies de dévelop pement (« business model ») des sites santé en France ;
— un « audit » en ligne de 59 sites de santé, destiné à évaluer l'application de la loi informatique et libertés (information des internautes sur leurs droits, dispositifs de sé curisation, déclaration...) et disposer ainsi d'une photographie, à un moment donné, de l'état de la protection des données en ce domaine.

A. Les contrôles sur place

Au cours des mois de novembre et de décembre 2000, des visites sur place ont été conduites auprès de 6 sites jugés significatifs en termes d'audience et de notoriété, selon une méthodologie identique, reposant en premier lieu sur une grille de questions systématiquement posées et orientées autour des thèmes suivants :
modalités d'élaboration du contenu rédactionnel ;
modèle économique du site et perspectives de développement (« business mo del ») ;
types de données à caractère personnel collectées, traitées et éventuellement cé dées ;
sécurités.

Il a également été procédé, outre le contrôle sur place des mesures de sécurité physiques et logiques — qui, globalement, sont apparues correctes —, à un certain nombre de tests destinés à vérifier la nature exacte et les modalités d'exploitation des données recueillies lors de la consultation du site.

1) PRESENTATION DES SITES

A l'exception de deux sites plus clairement orientés vers les professionnels de santé, les sites visités proposent à l'attention du grand public, sous la forme de dossiers thématiques, d'encyclopédies médicales, de guides de médicaments, de rubriques d'actualités, des informations pratiques portant non seulement sur la santé mais également sur des thèmes tels que la nutrition, la sexualité, ou encore la beauté, la forme et la psychologie. Ces sites comportent, pour la plupart, des rubriques de conseils personnalisés permettant aux internautes soit de poser des questions à des « experts » soit de répondre à des tests d'autoévaluation de l'état de santé. Enfin, les sites comportent généralement un forum de discussion et, pour certains, envoient régulièrement aux internautes, qui laissent leur mél, une lettre d'information. L'achat en ligne est embryonnaire (achat de micro-ordinateur, vente de parapharmacie...). 3 sites comportent une formule d'abonnement à un club.

Seul, un des 6 sites visités comporte un service de dossier de santé, rempli par l'internaute qui a la possibilité de garder l'anonymat.

Le mode d'élaboration des contenus des sites varie selon l'importance relative de l'équipe rédactionnelle, les partenariats éditoriaux, et bien sûr du type de services offerts.

Ainsi, certains sites font appel à des équipes rédactionnelles relativement étoffées composées de journalistes et de médecins salariés ou pigistes qui sont notamment chargés d'établir des dossiers thématiques et de rédiger les réponses aux questions posées par les internautes. Les contenus ainsi élaborés font l'objet d'une validation médicale interne avant d'être diffusés sur le site. D'autres privilégient l'achat de contenus auprès notamment de sociétés d'éditions médicales (par exemple, pour l'achat de contenus type encyclopédie médicale) et disposent alors d'une équipe rédactionnelle réduite.

Il doit être noté que toutes les sociétés visitées comportent à leur tête ou dans leur équipe au moins un médecin, certaines disposant également d'un comité scientifique apportant sa caution morale.

Tous les sites visités ont bénéficié d'investissements très significatifs. Outre les apports personnels, ces fonds proviennent essentiellement de sociétés de capital risque et des banques. Dans ce secteur, l'effet « start-up Internet » a donc aussi joué.

Or, aux dires mêmes des responsables des 6 sites visités, aucun n'a aujourd'hui atteint l'équilibre financier. Les résultats d'audience et les recettes escomptées de la revente de contenus et de la publicité n'ont, pour le moment, pas répondu aux attentes des promoteurs des sites, même si certains sites ont conclu des contrats avec des régies publicitaires (insertion de « bannières publicitaires » sur le site) ainsi que, pour un site (pour la partie réservée aux professionnels de santé), avec un laboratoire pharmaceutique.

Dans un contexte fortement concurrentiel qui voit l'audience générale des sites santé s'atomiser du fait de la multiplication des éditeurs, cette fragilité économique, qui n'est d'ailleurs pas spécifique à l'e-santé et que l'on retrouve chez toutes les jeunes entreprises de la net économie, se traduit par une attitude d'attentisme et de prudence, l'essentiel étant aujourd'hui, dans cette période de « turbulence » économique, de survivre et donc de réduire ses coûts de fonctionnement, de « se faire un nom sur la toile » (et de le garder), et de « flairer » les pistes de rentabilité possibles.

A cet égard, certains — se positionnant comme tiers de confiance (ou info-médiaires) — s'orientent d'ores et déjà vers une offre de dossier médical partagé entre l'internaute et le médecin et hébergé par le site ; la question du financement de ce type de services reste toutefois en suspens, plusieurs hypothèses étant avancées : paiement du service par les médecins, gratuité en contrepartie d'une utilisation des données par la société ou encore prise en charge du service par des entreprises ou des collectivités locales pour le compte de leurs salariés ou de leurs administrés.

En tout état de cause, ce contexte économique délicat explique pour partie le constat fait lors des visites, à savoir qu'aujourd'hui l'exploitation que font les sociétés des données personnelles collectées sur leur site est sinon inexistante du moins très réduite, et qu'elle ne semble pas constituer aujourd'hui une priorité, l'essentiel étant de survivre et pour cela de maintenir une certaine audience. Pour être tout à fait

complet, il doit être relevé que le respect de la confidentialité des données et de l'éthique médicale est souvent mis en avant par les sites comme un élément promotionnel.

2) LES TRAITEMENTS DE DONNÉES PERSONNELLES

Il convient de rappeler que les données personnelles susceptibles d'être collectées par les sites web comportent non seulement des informations dite « déclaratives » fournies par l'internaute (lorsqu'il complète un formulaire d'abonnement à une liste de diffusion, à un journal, à un club ou encore un questionnaire ou un dossier de santé) mais également des informations « perceptives », perçues lors de la visite de l'internaute. Il s'agit, d'une part, des informations issues du « bavardage » du protocole http spécifique au web telles que l'adresse IP de la machine qui se connecte, les documents demandés, la date et l'heure exactes ainsi que différentes données relatives aux logiciels utilisés. L'analyse de ces données enregistrées dans les journaux de connexion (fichier logs) permet d'élaborer des statistiques relatives par exemple aux pages les plus demandées, au temps passé sur chaque page, à la provenance géographique des internautes, à leur fournisseur d'accès, etc.

Ces données peuvent être corrélées avec un cookie déposé sur l'ordinateur de l'internaute. Dans ce cas, il s'agit d'obtenir des profils de navigation spécifiques à chacune des machines qui consultent le site afin de permettre la personnalisation du site pour l'internaute au fur et à mesure de sa navigation : il s'agira par exemple de présenter un article sur le traitement de la douleur à un internaute qui consulte une rubrique relative aux propriétés du paracétamol.

Cette personnalisation ne concerne pas uniquement le contenu rédactionnel du site mais vise également les messages publicitaires auxquels le site sert de support. Par exemple, une bannière publicitaire montrant le dernier numéro d'un magazine papier traitant de la douleur et des méthodes de relaxation permettant de la vaincre pourra être affichée sur l'écran de l'internaute qui demande l'article relatif aux propriétés du paracétamol.

Toutefois, les espaces publicitaires du site pourront être confiés en régie à une agence publicitaire qui se chargera de les commercialiser auprès d'annonceurs. Dans ce cas, lors de la première visite de l'internaute va se dérouler un processus dont l'internaute non averti n'a pas connaissance : certaines pages du site régi, notamment la page d'accueil, contiennent un marqueur (« tag ») qui demande au navigateur du visiteur de charger une image invisible présente non pas sur le site régi mais sur celui de la régie publicitaire.

Le navigateur de l'internaute va alors communiquer avec le serveur de la régie lui indiquant notamment qu'il arrive de tel site de santé. Dès lors, le serveur de la régie l'identifie comme un internaute intéressé par la santé et va lui servir une bannière ciblée en conséquence. En outre, le serveur de la régie dépose son propre cookie sur la machine de l'internaute. Grâce à ce cookie, elle va pouvoir le suivre et l'identifier dès lors que le même ordinateur se connectera sur un site dont elle gère l'espace publicitaire. Le site régi, comme la régie publicitaire elle-même, vont ainsi

collecter des profils sur les internautes qui vont s'affiner au fur et à mesure de leurs échanges avec lui.

Il s'agit là de techniques ordinaires sur Internet. L'internaute, comme la CNIL l'explique sur son site, peut évidemment refuser les cookies ou les effacer de son disque dur.

Que constate-t'on pour les 6 sites visités ?

Si l'ensemble des sites visités sollicitent le recueil de l'adresse e-mail (dès lors qu'il s'agit de recevoir une lettre d'information, de s'abonner à une liste de diffusion, de recevoir son mot de passe pour accéder à un service restreint...), en revanche, seuls ceux qui offrent des services réservés aux professionnels de santé ou proposent une formule d'abonnement à un club procèdent également à la collecte d'informations telles que le nom, l'adresse, parfois l'âge et la profession (pour les professionnels de santé), cette collecte étant présentée tantôt comme ayant un caractère obligatoire, tantôt un caractère facultatif. Le seul site proposant un dossier de santé en ligne prévoit que l'internaute s'identifie par un pseudo.

S'agissant de l'exploitation de ces données et de leur cession éventuelle, il convient de distinguer selon qu'il s'agit de sites grand public ou de sites réservés aux professionnels de santé ou offrant des services ouverts seulement à ces derniers.

En effet, s'agissant des sites grand public, tous les sites concernés ont indiqué ne procéder à aucune exploitation statistique, profilage à des fins commerciales ou cessions d'informations nominatives, contrairement d'ailleurs à ce qu'indiquent parfois leurs chartes de protection des données.

S'agissant de l'exploitation des données de navigation, tous les sites visités disposent d'outils standard pour établir leurs statistiques de fréquentation. Mais aucun n'a indiqué procéder à un rapprochement permettant de connaître l'identité de la personne profilée. Toutefois, il n'est pas à exclure qu'à l'avenir les « profils perceptifs » puissent être croisés avec des informations nominatives pour constituer des bases de prospects dans le cadre d'opérations de marketing direct.

Les 2 sites orientés vers les professionnels de santé ont indiqué disposer des moyens nécessaires pour procéder, sur la base des données communiquées par les professionnels de santé inscrits à leurs services et des données de connexion, à l'établissement de profils et de statistiques de fréquentation diffusées en particulier auprès de la régie publicitaire. Dans un cas, il a été précisé que les laboratoires pharmaceutiques étaient demandeurs d'informations nominatives sur les professionnels de santé.

En conclusion, si aujourd'hui l'exploitation à des fins commerciales des données directement ou indirectement nominatives recueillies sur les sites semble quasi-inexistante, la priorité étant, comme il a été indiqué, de privilégier l'accroissement de l'audience et, pour certains, la qualité du contenu rédactionnel, plusieurs sites n'ont pas dissimulé leur souhait de pouvoir, à terme, procéder à de telles exploitations surtout s'agissant des professionnels de santé, ce qui intéresse d'ailleurs au premier chef les laboratoires pharmaceutiques.

S'agissant des données susceptibles de révéler directement ou indirectement l'état de santé des internautes, qu'elles figurent sur un dossier de santé ou qu'elles puissent résulter de l'exploitation des données de navigation et en particulier se déduire de la consultation de telle ou telle page, les responsables des sites semblent prudents quant à l'éventualité d'une exploitation à des fins commerciales de ces données et surtout d'une cession, étant semble-t-il soucieux de donner au public l'image d'un site sérieux, éthique et garant de la confidentialité des informations ; certains n'ont ainsi pas hésité à créer des comités d'éthique, ou à établir des chartes dites éthiques...

Cependant, l'impression d'ensemble qui ressort des visites effectuées est que, dans cette période charnière que vit actuellement l'e-santé, les sites se contentent aujourd'hui d'« engranger » les données, ne sachant pas encore précisément comment et quand ils seront à même de les exploiter.

3) L'INFORMATION DES INTERNAUTES SUR LA PROTECTION DES DONNÉES PERSONNELLES

Sur ce point, et à l'égal des conclusions de l'audit des 60 sites (cf infra), force est de constater une disparité de situations tant sur la forme que sur le contenu de l'information délivrée aux internautes, aucun des 6 sites ne délivrant une information totalement satisfaisante.

Ainsi, si certains sites comportent des rubriques particulières, parfois très conséquentes, sur la protection des données, intitulées selon le cas « charte d'utilisation », « respect de la vie privée », « charte éthique », « charte de déontologie », « informations légales » d'autres en revanche ne donnent qu'une information succincte, se contentant d'un simple rappel des mentions prescrites par l'article 27 de la loi.

En tout état de cause, il doit être relevé à titre principal que la présence de ces rubriques, qui comportent parfois plusieurs pages, n'apporte pas toujours le niveau d'information que l'on serait en droit d'attendre de ce type de document : outre le fait que l'information délivrée peut être incomplète, les explications données ne sont pas toujours compréhensibles et sont quelquefois contradictoires.

S'agissant plus précisément du contenu de l'information sur la protection des données, il doit être souligné que tous les sites visités indiquent, mais de façon quelque peu éparpillée, l'identité du responsable du site, précisent le caractère obligatoire ou facultatif de la collecte, le lieu où s'exerce le droit d'accès, donnent une information spécifique sur l'utilisation faite des données de santé collectées (excepté pour un site qui toutefois ne collecte des informations qu'auprès des professionnels de santé). 4 sites sur 6 indiquent ne faire qu'un usage purement interne des données. Peu de sites informent les internautes sur la présence de cookies et la façon de les désactiver.

B. L'évaluation de 60 sites de santé : une situation contrastée mais très largement insatisfaisante

Suivant la méthodologie adoptée lors de l'opération « 100 sites de commerce électronique » réalisée au début de l'année 2000, il a été procédé, à partir d'une grille d'une centaine de questions, à l'évaluation, en ligne, de 59 sites web, les critères de choix des sites étant dictés par la volonté d'avoir une vision globale et diversifiée du secteur étudié (institutionnels, laboratoires pharmaceutiques, sociétés commerciales, presse médicale, associations de patients, sociétés savantes, associations de médecins et syndicats de professionnels de santé).

1) LES ENSEIGNEMENTS

L'information des internautes sur leurs droits est très largement insatisfaisante

Sur l'ensemble des sites audités, 43 ont fait l'objet d'un déclaration à la CNIL. Le taux de déclaration (71 %) est supérieur à celui qui avait été constaté au printemps 2000 dans le cadre de l'opération d'audit des 100 sites de commerce électronique.

Toutefois, ce résultat ne doit pas faire illusion. En effet, sur les 51 sites qui collectent des données personnelles, seuls 30, soit 58 %, comportent une information sur la vie privée et les données personnelles ou une mention sur la loi « informatique et libertés ». Lorsque cette information est réalisée, elle n'est mentionnée sur tous les supports de collecte que dans un cas sur trois. Dans 36 % des cas (11 sites sur 51), les sites consacrent une rubrique particulière à la protection des données. La fréquence des mentions d'information est cependant plus forte quand le site a été déclaré à la CNIL (62 %) que quand il ne l'est pas (19 %).

Dans la terminologie utilisée, la notoriété de la loi du 6 janvier 1978 ou de la loi « Informatique et Libertés » est très forte, ce qui confirme les enseignements de l'opération menée sur les sites de commerce électronique.

Il demeure qu'au total et s'agissant de l'information des personnes, la situation est très insatisfaisante.

Elle l'est plus encore s'agissant du contenu de cette information.

Ainsi, seuls 1/3 des sites donnent en page d'accueil une information sur le nom et la qualité du responsable du site, bien que les éditeurs de sites soient désormais tenus de mettre cette information à la disposition du public en application de l'article 40-10.1 de la loi du 1er août 2000 et de la directive européenne du 24 octobre 1995.

Seuls 30 % des sites indiquent clairement le caractère facultatif ou obligatoire des informations collectées et 37 % seulement indiquent le lieu d'exercice du droit d'accès (ce pourcentage était de 48 % à l'issue de l'évaluation des 100 sites français de commerce électronique, pourcentage déjà considéré comme insuffisant).

S'agissant de l'utilisation des données, 25 % précisent expressément que les données collectées sont à usage purement interne. 20 % des sites informent les internautes d'une possible communication des données collectées à des tiers. Il en résulte que dans *55 %* des cas, les internautes ne sont pas informés de l'utilisation de leurs données.

Toutefois, lorsqu'il est précisé que les données peuvent être adressées à des tiers, il est également indiqué que l'on peut s'opposer à une telle cession.

On notera également que 44 % des sites font état de l'existence de partenariats et que la même proportion comporte des bandeaux publicitaires en ligne.

Enfin, la présence de cookies, constatée dans 62,7 % des sites, ne s'accompagne d'une information sur leur utilisation éventuelle que dans 10 % des cas.

2) LES ÉLÉMENTS PLUS POSITIFS : L'ÉMERGENCE D'UNE SPÉCIFICITÉ DES DONNÉES DE SANTÉ

15 sites sur les 31 classés comme sites grand public délivrant des conseils de santé, soit 48,3 %, comportent une information spécifique des internautes sur l'utilisation des données de santé que ces derniers sont amenés à communiquer au site. Cette rubrique peut prendre la forme d'une information sur l'usage purement interne des données dans 7 cas sur 15, d'une information sur les mesures de confidentialité adoptées dans 6 cas sur 15 et d'une information sur la validation scientifique du site dans 7 cas sur 15.

Il convient également de relever que dans 11 cas sur 15, les sites comportent un avertissement appelant l'attention des internautes sur le fait que les informations délivrées ne remplacent pas une consultation médicale.

Lorsqu'une information spécifique est ainsi réalisée, elle s'accompagne dans 40 % des cas du recueil du consentement de l'internaute soit à l'utilisation de ses données, soit à la cession de ses données à des tiers.

Par ailleurs, une quinzaine de sites font état d'un procédé de sécurisation : certains par l'indication dans la barre du logiciel de navigation d'une icône spécifique, d'autres précisent le procédé technologique et/ou le nom de l'organisme certificateur. 6 sites seulement laissent la possibilité à l'internaute de garder l'anonymat par un pseudo ou un numéro.

Il doit enfin être souligné que 10 sites sur le total font mention de l'adhésion à une charte éthique ou à un label. Or, la déclaration d'adhésion à une charte ou à un label n'a pas exactement comme corollaire un respect effectif des règles de protection des données.

En effet, sur ces 10 sites, si 9 sont déclarés à la CNIL, 7 seulement délivrent une information sur la protection des données, ce qui semble indiquer que la déclaration d'adhésion à une charte ne se traduit pas toujours dans les faits par un respect effectif des engagements contenus dans ces chartes.

Cela pourrait également signifier que les chartes auxquelles il est fait référence, du fait de leur caractère peu contraignant et surtout de l'imprécision de leurs recommandations, ne satisfont pas à l'obligation de clarté vis-à-vis des internautes...

En conclusion, ces statistiques révèlent, semble-t-il, l'émergence, dans le monde de l'Internet santé, d'une certaine prise de conscience des responsables des sites de santé quant à la nécessité de reconnaître aux données de santé un statut particulier et de leur faire bénéficier d'un régime de protection spécifique. Mais cette évaluation atteste aussi un certain « fossé éthique » entre les sites particulièrement protecteurs, prudents et respectueux de la loi et d'autres qui paraissent très largement ignorer la loi du 6 janvier 1978 et la spécificité des données médicales.

C'est la raison pour laquelle la CNIL a souhaité tirer la sonnette d'alarme et a décidé d'engager vis-à-vis des responsables de sites de santé une action pour assurer un meilleur respect des règles de protection des données, s'agissant tout particulièrement de l'information des internautes qui doivent être assurés que le service qui leur est proposé sur le net — qu'il s'agisse de la délivrance de conseils, de tests d'autoévaluation, de la tenue d'un dossier de santé — non seulement leur délivre une information de qualité mais est licite et leur garantit que les données qu'ils communiquent sur leur état de santé ne seront pas divulguées.

Nonobstant les initiatives déjà prises en ce domaine par différents acteurs, la CNIL a ainsi estimé nécessaire d'établir des recommandations spécifiques à l'attention des sites de santé.

C. La recommandation de la CNIL du 8 mars 2001

1) LES INITIATIVES DÉJà PRISES

A l'étranger, principalement aux Etats-Unis et en Suisse, des initiatives ont été prises pour définir des chartes de qualité[16] dont aucune cependant ne s'appuie précisément sur les législations de protection des données existantes ou sur une procédure de labellisation reconnue. S'agissant de la protection des données, les chartes mettent généralement l'accent sur deux principes : le respect de la confidentialité des informations personnelles concernant les visiteurs des sites, l'obligation d'une information claire des internautes et du recueil de leur consentement à l'utilisation de leurs données, le droit d'accès étant généralement mentionné. Mais sauf exception (le guide de l'AMA), ces chartes ne comportent pas de recommandations pratiques.

[16] La *charte Heath On the Net* (dite « Hon code ») : cette charte, la plus connue, a été élaborée en 1996 par une association suisse, en concertation avec des professionnels de santé, des éditeurs de sites et des groupes de patients, *la charte Hi-ethics :* il s'agit d'une initiative, prise en 1999, par les 20 sites santé et tournisseurs de contenu les plus consultés sur Internet (essentiellement américains), *la charte Internet Healthcare Coalition :* la « eHealth code of Ethics » a été créée en 1997 par une association réunissant fournisseurs de contenu et consommateurs en réponse à une demande des consommateurs de pouvoir disposer d'informations fiables en matière de santé sur Internet et d'une demande d'intervention de la part de l'industrie pour mettre en place des standards internationaux applicables aux sites santé, *les quidelines for médical and Health Information Sites on the Internet :* ces recommandations établies par l American Médical Association (AMA), l'équivalent du Conseil de l'ordre, sont relatives aux sites de l'AMA, mais elles se veulent également un guide à l'intention des créateurs de sites consacrés à la santé.

Dans le cadre du programme « e-europe » 2002, la Commission européenne a engagé une action spécifique sur l'e-santé qui vise notamment, sur la base des corpus de règles déjà existantes, à promouvoir des critères de qualité de sites de santé susceptibles de déboucher sur des procédures de labellisation nationales.

En France, le Conseil national de l'ordre des médecins a établi en avril 2000 une charte déontologique puis, en juin et en octobre 2000, deux rapports consacrés à l'exercice médical et Internet. Enfin, l'Ordre a récemment adopté un modèle de clause à insérer dans les contrats que concluent les médecins collaborant à des sites Internet. Ce contrat précise notamment que si la société entend tirer des statistiques et les exploiter à partir des informations recueillies, celles-ci ne doivent pas permettre l'identification des personnes auxquelles elles se rapportent.

Une charte pour la communication sur Internet des entreprises pharmaceutiques a également été conclue le 26 décembre 2000 entre l'Agence française de sécurité sanitaire des produits de santé (AFSSAPS) et le Syndicat national de l'industrie pharmaceutique (SNIP), afin d'aider les entreprises pharmaceutiques à concevoir leurs pages Internet dans le respect de la réglementation. Il doit être rappelé en effet qu'en France, la publicité auprès du grand public, sous contrôle de l'AFSSAPS, ne peut concerner que des médicaments qui ne sont ni soumis à prescription médicale obligatoire, ni remboursables par la sécurité sociale et dont l'AMM ne comporte aucune restriction en matière de publicité auprès du public. La publicité de médicaments auprès des professionnels de santé est, elle, permise mais soumise à des conditions restrictives quant au contenu et à sa diffusion et doit faire l'objet d'un dépôt auprès de l'AFSSAPS.

Dès lors, la charte préconise que des restrictions d'accès (attribution de mots de passe après avoir vérifié la qualité du professionnel) soient mises en place pour réserver aux seuls professionnels de santé la publicité des médicaments sur Internet. Outre des recommandations précises sur le contenu de l'information que peuvent délivrer les entreprises, la charte comporte une rubrique « profilage » où il est indiqué que « le profilage, à l'insu de l'internaute (c'est-à-dire le professionnel de santé), n'est pas autorisé dans le cadre des sites pharmaceutiques, c'est-à-dire que les pages promotionnelles affichées ne doivent pas varier en fonction du profil de l'internaute. » Il est toutefois précisé que « sur demande de l'internaute, ce profilage est autorisé ».

Enfin, un groupe de travail, auquel la CNIL participe, a été constitué à l'initiative du ministère de l'Emploi et de la Solidarité et du Conseil national de l'ordre des médecins en vue de l'élaboration d'une charte éthique et de transparence, susceptible de déboucher, à terme, sur une labellisation et une certification des sites « e-santé ».

Deux démarches sont envisagées :
— la conception, sous la forme d'un site web, d'un espace de formation et d'information des internautes appelés à consulter des sites santé, leur offrant la possibilité d'obtenir en un seul lieu tous les renseignements nécessaires leur permettant d'être mieux informés de leurs droits, de savoir qui fait quoi, où s'adresser en cas de difficul-

tés, et les incitant à vérifier, sur la base d'un référentiel de qualité, si le site respecte ses engagements et peut être considéré comme un site fiable.
— l'élaboration dudit référentiel de qualité ainsi que d'une méthode de vérification, de « marquage » des sites et d'évaluation qui pourrait être assurée par une structure pérenne type association, regroupant l'ensemble des acteurs concernés.

2) LES RECOMMANDATIONS PRATIQUES DE LA CNIL

Les multiples possibilités de collecte des informations qu'offre Internet rendent indispensable la transparence dans le traitement et l'utilisation de ces données. Ainsi, il est impératif que les internautes appelés à consulter des sites de santé soient clairement informés de l'usage fait de leurs données, des destinataires de celles-ci et de leurs droits.

Le souci d'assurer une meilleure application de la loi par les sites de santé a ainsi conduit la Commission à faire œuvre de pédagogie et à émettre, à l'attention des responsables de ces sites, de nombreuses recommandations pratiques pour informer concrètement les internautes de leurs droits, s'agissant en particulier de l'indication, dès la page d'accueil, de la raison sociale et du siège social du site et de l'identité de la personne désignée pour assurer le respect des règles de protection des données, du contenu de la rubrique « Informatique et Libertés/Protection des données personnelles », des conditions d'utilisation des données, de la durée de conservation des informations directement nominatives et des données de connexion, des conditions d'exercice du droit d'accès, des mesures de sécurité... Compte tenu des risques de divulgation et d'utilisation détournée des informations inhérents au réseau Internet, la confidentialité des informations médicales nominatives appelées à circuler sur le réseau doit en effet pouvoir être garantie par le recours systématique à des moyens de chiffrement.

Mais la Commission a également souhaité réaffirmer, comme elle l'avait fait lors de sa recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel, que les données de santé revêtant un caractère directement ou indirectement nominatif, qu'elles aient été communiquées au site par l'internaute et/ou par un professionnel de santé, doivent faire l'objet d'une protection particulière et ne doivent pas pouvoir être exploitées à des fins commerciales ni transmises à quiconque à des fins commerciales ou de prospection commerciale.

Il doit, à cet égard, être rappelé que la directive européenne en son article 8, prévoit que les États membres interdisent le traitement des données relatives à la santé, sauf si le traitement est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration des soins ou de traitements ou de la gestion de services de santé (situations dont ne relèvent pas à l'évidence les sites santé grand public) et si la personne concernée a donné son consentement explicite à un tel traitement, sauf dans les cas, indique la directive, « où la législation de l'État membre prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée ».

Mais qu'entend-on par donnée de santé ? Comment, en particulier, doit-on considérer l'e-mail et/ou le nom et l'adresse laissés par un internaute sur un site de santé ou encore l'exploitation sous une forme nominative de données de navigation sur un site de santé spécialisé dans une pathologie déterminée ?

Certes, il serait excessif de considérer que parce qu'un internaute a consulté tel ou tel site sur le diabète ou le SIDA, le traitement de ses données de navigation doit être considéré comme un traitement de données relatives à son état de santé. Ceci révèle tout au plus un intérêt pour la pathologie en question.

Néanmoins, le traitement des données de connexion associées à l'adresse e-mail ou au nom de l'internaute, s'il ne révèle pas en tant que tel l'état de santé de l'internaute, revêt toutefois une sensibilité particulière et une certaine vigilance s'impose.

En effet, si de telles données issues des consultations des pages des sites web étaient associées à des informations nominatives, il serait à craindre qu'elles puissent être utilisées à des fins étrangères à l'intérêt de l'usager.

En conséquence, la Commission a estimé que les internautes devraient être clairement informés des finalités poursuivies, et que toute exploitation nominative des données de navigation ainsi que toute cession à des tiers de telles données devraient être subordonnées au consentement exprès de la personne concernée, recueilli par le biais d'une case à cocher.

Au-delà de ces recommandations, la Commission a souhaité appeler l'attention des pouvoirs publics sur la nécessité d'une part, de poser expressément dans la loi le principe de l'interdiction de toute commercialisation de données de santé directement ou indirectement nominatives et d'autre part, compte tenu de la possibilité désormais offerte par des sociétés de service d'assurer l'hébergement de dossiers de santé, accessibles par Internet, de prévoir des garanties sérieuses de nature à prévenir tout risque de divulgation ou d'utilisation indues des données et d'envisager, le cas échéant, une procédure d'agrément de tels organismes.

Délibération n° 01-011 du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public

La Commission nationale de l'informatique et des libertés, Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et notamment son article 6 ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et notamment en son article 8 ;

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

Vu les articles 226-13 et 226-14 du code pénal relatifs au secret professionnel ;

Vu le code de la santé publique ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978, et notamment son article premier ;

Vu le décret n° 95-100 du 6 septembre 1995 portant code de déontologie médicale ;

Vu la délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel ;

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

La Commission considère que la mise en œuvre des sites web consacrés à la santé répond à un besoin légitime d'information du public. Toute personne consultant un tel site doit se voir garantir la délivrance d'une information de qualité mais aussi la protection de ses données personnelles. La Commission a procédé à l'évaluation de sites de santé et à plusieurs vérifications sur place afin d'apprécier l'application des règles de protection des données par les sites de santé. Elle a constaté que les dispositions de la loi du 6 janvier 1978 ne sont pas appliquées de manière satisfaisante, s'agissant notamment de l'information des internautes sur l'utilisation qui peut être faite de leurs données et sur leurs droits.

Les données de santé à caractère personnel, parce qu'elles relèvent de l'intimité de la vie privée, doivent faire l'objet d'une protection particulière, exigée tant par l'article 6 de la convention n° 108 du Conseil de l'Europe que par l'article 8 de la directive européenne du 24 octobre 1995. A cet égard la Commission réaffirme la pertinence de sa recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel : les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et à des fins de santé publique, dans les conditions définies par la loi.

Les données de santé revêtant un caractère directement ou indirectement nominatif, qu'elles aient été communiquées au site par l'internaute et/ou par un professionnel de santé, ne devraient pas pouvoir être exploitées à des fins commerciales ni transmises à quiconque à des fins commerciales ou de prospection commerciale. Le respect de ce principe devrait s'imposer aux sites web de santé appelés à recueillir des données nominatives de santé mais aussi aux sociétés et organismes susceptibles de gérer et de conserver, pour le compte de professionnels de santé ou d'établissements de santé, des dossiers médicaux accessibles sur Internet.

Le traitement des données de connexion associées à des données nominatives telles que l'adresse e-mail ou le nom de l'internaute, si elles ne révèlent pas en tant que telles l'état de santé de l'internaute, revêtent toutefois une sensibilité particulière. En effet, si de telles données issues des consultations des pages des sites web, étaient associées à des informations nominatives, il serait à craindre qu'elles puissent être utilisées à des fins étrangères à l'intérêt de l'usager (compagnies d'assurance, employeurs, banques...). En conséquence les internautes devraient être clairement informés des finalités poursuivies et toute exploitation nominative des données de navigation ainsi que toute cession à des tiers de telles données devraient être subordonnées au consentement exprès de la personne concernée, recueilli par le biais d'une case à cocher.

Enfin, compte tenu des risques de divulgation et d'utilisation détournée des informations inhérents au réseau Internet, la confidentialité des informations médicales nominatives appelées à circuler sur le réseau devrait être garantie par le recours systématique à des moyens de chiffrement.

Le souci d'une meilleure application de la loi par les sites de santé conduit la Commission à recommander la mise en oeuvre des mesures suivantes.

Indication de la raison sociale et du siège social du site

L'indication de la raison sociale et du siège social du site devrait apparaître clairement dès la page d'accueil ou dans une rubrique accessible dès la page d'accueil (par exemple sous le titre « Qui sommes-nous »).

En outre, l'identité de la personne désignée pour assurer le respect des règles de protection des données et en particulier de la confidentialité des données de santé devrait être précisée.

Création d'une rubrique « Informatique et Libertés/Protection des données personnelles »

Une rubrique d'information devrait être conçue de façon distincte sous un titre spécifique et être accessible dès la page d'accueil. Le texte de cette rubrique devrait être concis et rédigé clairement, afin d'être compréhensible par chacun. Le responsable du site devrait y indiquer :

1) Qu'en France et en Europe les données personnelles de santé sont protégées par la loi (article 226-13 du code pénal, loi du 6 janvier 1978, directive européenne du 24 octobre 1995).

Qu'au cours de la navigation sur le site, selon les pages visitées ou les services qui intéressent l'internaute, il pourra être amené à communiquer des informations le concernant susceptibles de révéler son état de santé.

Que les données de santé revêtant un caractère directement ou indirectement nominatif, qu'elles aient été communiquées par l'internaute et/ou par un professionnel de santé, ne font l'objet d'aucune exploitation commerciale et ne sont transmises à quiconque à des fins commerciales ou de prospection commerciale.

2) Si les données collectées auprès de l'internaute ou résultant de sa naviga tion sur le site sont réservées à un usage strictement interne ou non.

3) Quel usage sera fait de l'adresse e-mail et/ou des coordonnées (nom et/ou adresse) de l'internaute dans le cas où ceux-ci sont collectés.

4) Qu'en aucun cas la cession ou la mise à disposition à des tiers, à des fins commerciales, de l'adresse e-mail ou des coordonnées de l'internaute, (à l'exclusion de toutes données relatives à l'état de santé réel ou présumé de ce dernier) ne pourra être opérée sans qu'il ait été préalablement mis en me sure de s'y opposer, par le biais d'une case à cocher.

5) Que l'internaute qui aura communiqué son adresse e-mail et/ou ses coor données pourra à tout moment se faire radier de tout fichier et de tout traite ment auxquels ces informations ont donné lieu.

6) Si les données de connexion seront ou non exploitées sous une forme di rectement nominative ou non.

7) Quelles exploitations éventuelles des données de connexion sous une forme nominative sont réalisées.

Dans une telle hypothèse, il devrait être précisé à l'internaute si ces données sont ou non susceptibles d'être mises à la disposition de tiers, notamment à des fins commerciales.

Dans les deux cas, une telle exploitation des données de connexion associées à des données nominatives ne peut être réalisée qu'avec l'accord des personnes, recueilli par le biais d'une case à cocher.

8) Lorsque des cookies sont utilisés, les buts poursuivis par leur mise en oeuvre ainsi que les conséquences de leur désactivation par l'internaute.

9) La durée de conservation des informations directement nominatives (adresse e-mail, coordonnées, données de santé, autres...) ainsi que la durée de conservation des données de connexion. Ces durées doivent être li mitées et proportionnées aux finalités du traitement de telles données.

10) Les coordonnées ou l'adresse e-mail du service ou du correspondant en charge de répondre aux demandes de droit d'accès, de rectification et de suppression présentées par les internautes. Ce droit devrait pouvoir s'exer cer à tout moment en ligne.

Collecte directe de données auprès de l'internaute

Toute collecte directe de données auprès de l'internaute (sous forme ou non de questionnaire) devrait être accompagnée d'une information précisant, sur le support de collecte, le caractère obligatoire ou facultatif du recueil de chaque information demandée (par exemple par le biais d'un astérisque).

Dans l'hypothèse où il est envisagé de mettre à la disposition ou de céder à des tiers à des fins commerciales des données telles que l'adresse e-mail ou les coordonnées de l'internaute, à l'exclusion de toutes données relatives à l'état de santé réel ou présumé de ce dernier, l'internaute doit être mis en mesure de pouvoir s'y opposer en ligne par le biais d'une case à cocher devant figurer sur le support de collecte.

A défaut d'une telle mention sur le support de collecte, les données seront supposées être destinées à un usage exclusivement interne.

Mesures de confidentialité et de sécurité

Des mesures de sécurité reposant notamment sur le recours à des moyens de chiffrement ainsi que sur des dispositifs de journalisation des connexions devraient être mises en place pour assurer l'intégrité et la confidentialité des données.

Le contrat passé avec un hébergeur tiers devrait comporter des clauses prévoyant les nécessaires mesures destinées à assurer la sécurité des données, ainsi que leur seuls accès et utilisation par des personnes habilitées à en connaître.

Ces mesures doivent être portées à la connaissance de la CNIL lors de l'accomplissement des formalités préalables.

Forum de discussion

Une mention d'information devrait préciser que l'espace de discussion est destiné à permettre aux internautes d'apporter leur contribution aux thèmes de discussion proposés et que les données qui y figurent (adresse e-mail et/ou coordonnées notamment) ne peuvent être collectées ou utilisées à d'autres fins, et tout particulièrement à des fins commerciales ou de prospection.

Il est recommandé qu'un modérateur soit chargé de supprimer les contributions susceptibles d'engager la responsabilité du site ou de porter atteinte à la considération ou à l'intimité de la vie privée d'un tiers.

La possibilité de participer au forum sans avoir à s'identifier devrait être offerte à l'internaute, notamment lorsque l'espace de discussion comporte un modérateur.

Les intervenants devraient être informés de leur droit de demander à tout moment la suppression de leurs contributions en s'adressant au service en charge du droit d'accès.

Le développement des sites de santé sur Internet conduit la Commission à souhaiter que le principe de l'interdiction de toute commercialisation de données de santé directement ou indirectement nominatives soit posé par la loi, comme l'est déjà, dans le code de la santé publique, l'interdiction d'utiliser à des fins de prospection commerciale des données relatives aux prescriptions des médecins lorsqu'elles revêtent à leur égard un caractère directement ou indirectement nominatif.

Par ailleurs la possibilité désormais offerte par des sociétés de service d'assurer l'hébergement de dossiers de santé, accessibles par Internet, conduit la Commission, à appeler l'attention des pouvoirs publics sur la nécessité de prévoir des garanties sérieuses de nature à prévenir tout risque de divulgation ou d'utilisation indue des données et d'envisager, le cas échéant, une procédure d'agrément de tels organismes.

II. MON E-DOSSIER

Dans le prolongement du rapport sur le développement des sites de santé en France, la Commission a examiné, lors de sa séance du 8 mars 2001, quatre projets de dossier médical sur Internet, projets qui illustrent de façon significative les perspectives d'évolution de l'Internet médical en France.

Certes, le phénomène du développement sur Internet de réseaux d'informations médicales n'est pas nouveau et la Commission a déjà eu, à plusieurs reprises, l'occasion de se prononcer sur de tels projets. Elle a notamment rendu des avis en 1997 et 1998 sur la mise en place de réseaux ville-hôpital sur Internet.[17]

[17] Délibérations n° 97-049 du 24 juin 1997 et n° 98-022 du 17 mars 1998 (centres hospitaliers d'Annecy et d'Armentières), 18° et 19° rapports d'activité.

Toutefois, ces projets soulèvent des interrogations nouvelles qui tiennent d'une part, à l'intervention de sociétés commerciales dans la gestion du dossier de santé et d'autre part, au rôle plus actif confié à l'usager du système de soins dans les dispositifs d'information proposés. Dans les quatre projets en effet, c'est l'usager qui va décider de la création de son dossier et autoriser ou non son accès aux professionnels de santé. Dès lors, se pose la question des conditions dans lesquelles il pourra lui-même accéder au contenu de son dossier.

A. Présentation des projets

1) 1) LES RÉSEAUX VILLE-HÔPITAL DE L'ASSOCIATION POUR LA BONNE COORDINATION MÉDICO-CHIRURGICALE ET DE L'ASSOCIATION INTÉGRALE SANTÉ DE LENS

Ces associations qui regroupent des professionnels de santé hospitaliers et libéraux ont pour objet de mieux coordonner la prise en charge médico-chirurgicale de patients adultes.

Pour assurer cette coordination, ces réseaux se sont dotés d'une application informatique qui devrait permettre la constitution, pour les patients hospitalisés et dont le suivi médical est effectué en ville, d'un dossier de santé électronique sécurisé (« coffre-fort électronique ») accessible sur Internet sous certaines conditions, aux malades et aux différents professionnels de santé appelés à assurer leur suivi tant à l'hôpital qu'en ville. Ce dossier multimédia a vocation à comporter non seulement les observations, prescriptions, résultats d'examens, diagnostics et traitements mais également des radiographies, scanners, échographies, IRM...

Les dossiers seront physiquement hébergés sur un serveur géré par une société de service et de conseil.

Ces projets bénéficient de financements de l'AP-HP (pour l'Hôtel-Dieu), de l'assurance maladie et d'institutions de prévoyance.

2) LE PROJET DE LA SOCIETE USIS-URGENCE : LA GESTION D'UN DOSSIER D'URGENCE MÉDICALE SUR INTERNET

Ce projet, présenté par une société américaine, vise à offrir à l'usager la possibilité de créer un dossier de santé accessible par Internet et a *priori* limité aux données médicales nécessaires en cas de situation d'urgence — qu'il peut ou non faire valider par le professionnel de santé de son choix. C'est un service qui pourrait être proposé en France, par exemple aux personnes appelées à voyager fréquemment, dans le cadre de la souscription de contrats d'assistance, la société ne jouant alors qu'un rôle de prestataire technique.

Il convient de noter que des services analogues existent déjà en France.

L'usager serait doté d'une carte personnelle qui, selon les cas, pourrait revêtir plusieurs formes : carte à puce spécifique réalisée au nom de la société qui propose ce service, intégration du service dans une carte bancaire, voire même possibilité d'utiliser la carte vitale. En l'absence de carte, l'accès au serveur serait également possible à l'aide d'un code d'accès numérique et d'un mot de passe alphanumérique.

L'usager pourrait faire valider ses données en demandant, par messagerie électronique, au médecin de son choix, d'y accéder pour les vérifier (l'adjonction du symbole du caducée matérialiserait cette validation). Tout professionnel de santé, où qu'il soit dans le monde, pourrait alors se connecter au site web détenant les dossiers d'urgence et consulter les données après avoir saisi le numéro d'identification du patient figurant sur la carte de l'usager (dans le cas où celui-ci serait dans l'incapacité physique de fournir ces informations).

La base de données serait hébergée en France.

3) LE PROJET DE LA SOCIETE UNI-MEDECINE : UN SERVICE DE GESTION DES DOSSIERS PROPOSÉ AUX USAGERS ET AUX PROFESSIONNELS DE SANTÉ

Le projet présenté par la société Uni-Médecine consiste à proposer un service qui permettrait aux patients de donner accès par Internet à leur dossier médical aux médecins de leur choix en les y habilitant à l'aide d'une clé (mot de passe).

Ce service serait dans un premier temps offert gratuitement aux usagers et aux professionnels de santé. Mais Uni-Médecine commercialise également ce service auprès de promoteurs de réseaux de soins.

L'usager ouvrirait l'accès de son dossier médical aux médecins de son choix, en leur communiquant à cet effet son mot de passe. Seul le médecin ainsi « agréé » pourrait prendre connaissance du dossier médical. Un médecin « non agréé » par le patient qui souhaiterait mettre une information dans le dossier pourrait le faire, et deviendrait de ce fait « médecin candidat », sans pour autant pouvoir lire aucune des informations figurant dans le dossier : il se verrait conférer un droit d'écriture sans disposer pour autant d'un droit de lecture.

B. Les conditions d'accès au dossier médical sur Internet : vers une maîtrise des informations médicales par le patient ?

1) LA CONSTITUTION DU DOSSIER PAR L'USAGER ET LES MODALITÉS D'ACCÈS AUX INFORMATIONS

Les projets soumis à la Commission ont pour caractéristique commune de placer l'usager au coeur du dispositif d'information. Dans tous les cas, son consente-

ment exprès sera en effet nécessaire pour permettre la création du dossier de santé, ses modalités d'intervention sur les données différant cependant d'un projet à l'autre.

Dans le projet présenté par Uni-Médecine, l'usager décide de la création de son dossier de santé sur Internet, autorise les professionnels de santé de son choix à ouvrir son dossier et à le lire et à le mettre à jour, mais ne peut consulter directement par Internet son dossier médical puisqu'il doit passer par l'intermédiaire du professionnel de santé de son choix pour accéder à ses informations.

Dans les projets de l'Association pour la bonne coordination médico-chirurgicale et de l'Association Intégrale Santé de Lens, le médecin hospitalier traitant constitue, avec l'accord exprès du patient, le dossier de santé, mais c'est le patient qui donne à ce médecin son accord pour que tel ou tel autre professionnel de santé du réseau accède à son dossier médical. Toutefois, c'est le médecin qui dispose de l'option technique lui permettant d'ouvrir le dossier à d'autres professionnels de santé (cette option s'accompagnant de l'apparition systématique d'un message l'avertissant de la nécessité d'obtenir le consentement libre et éclairé du malade). Le patient peut accéder directement par Internet à certaines parties de son dossier médical et en particulier à une fiche qui comporte des données d'alerte médicales, l'identité des médecin (s) traitant (s) et à un aide-mémoire personnel que lui seul peut visualiser. Le dossier de santé comporte également une fiche de liaison détaillant les événements médicaux le concernant : diagnostics, nature, dates et résultats des examens pratiqués, opérations effectuées, traitements suivis, etc., informations dont l'accès ne lui est reconnu qu'après accord du médecin auteur de l'information.

Dans le projet Usis-Europe, l'usager crée son dossier de santé, fait valider les informations médicales retenues par le professionnel de santé de son choix, et peut consulter directement son dossier sur Internet et le modifier. Il est toutefois prévu qu'au cas où il modifierait une information ayant fait l'objet d'une validation médicale, un message d'alerte apparaisse pour préciser que l'information n'est plus validée sur le plan médical.

Ainsi qu'il peut être constaté, les modalités d'intervention du patient ou de l'usager dans son dossier de santé diffèrent selon les projets, s'agissant en particulier de son droit d'accès.

Or, la possibilité ainsi ouverte à chacun de pouvoir décider de la création d'un dossier de santé accessible en temps réel sur Internet, de déterminer les professionnels de santé qui pourront y accéder et de pouvoir fixer l'étendue des autorisations d'accès ne doit-elle pas logiquement s'accompagner de la reconnaissance d'un droit d'accès direct de la personne aux informations médicales la concernant ?

N'y aurait-il pas, en effet, une contradiction à vouloir offrir à l'usager les moyens de décider du support et des modalités de communication de son dossier de santé sans lui en donner la maîtrise complète ? La nécessité, reconnue dans tous les projets soumis à la Commission, de recueillir le consentement de la personne préalablement à toute inscription ou communication d'informations médicales n'apparaît-elle pas dénuée de signification si la personne ne peut pas connaître elle-même le contenu de l'information dont elle est sensée commander les accès ?

Certes, la législation actuelle, et en particulier l'article 40 de la loi du 6 janvier 1978, prévoit que l'accès au dossier médical s'exerce par l'intermédiaire d'un médecin que l'intéressé désigne à cet effet, cette médiation devant permettre au médecin d'apprécier conformément au code de déontologie si tout ou partie seulement des informations contenues dans le dossier médical pourront être communiquées au malade. Mais ce passage obligé par un médecin est trop souvent perçu par le malade comme un obstacle de plus dans la communication de son dossier médical alors qu'il devrait plutôt se concevoir comme un moyen pour le médecin d'expliquer au malade, dans un langage compréhensible, la teneur de son dossier.

Or, l'irruption des nouvelles technologies de l'information et en particulier d'Internet dans cette problématique de l'accès au dossier médical incite plus que jamais à repenser les relations médecin-malade en termes nouveaux : le malade accepte de moins en moins son rôle passif de « patient » et revendique, aussi en ce domaine, le droit à l'information.

Ainsi, les associations de défense des droits des patients, que la CNIL a consultées sur ce point, se déclarent bien entendu favorables à la reconnaissance d'un accès direct par l'usager à ses informations de santé qui, selon elles, doit être inconditionnel, concerner l'ensemble des données médicales et s'exercer quel que soit le support, y compris donc Internet.

Les médecins eux-mêmes, et en particulier l'Ordre national des médecins, reconnaissent la nécessité de faire évoluer le droit et les pratiques, tout en soulignant les précautions à prendre pour certaines pathologies sensibles (psychiatriques) et les aménagements à prévoir s'agissant en particulier de leurs notes personnelles dont l'accès devrait leur être réservé.

Les pouvoirs publics, conscients de cette évolution des mentalités, s'orientent, comme on le sait, vers une reconnaissance d'un droit d'accès direct au dossier médical et en conséquence vers une modification de la loi.

Pour sa part, la CNIL a déjà eu l'occasion dans le passé de prendre position sur le sujet. Lors de l'examen des premiers projets expérimentaux de cartes de santé lancés en France dans le milieu des années 1980, la CNIL avait ainsi estimé que la nécessité de recueillir l'accord des patients et de leur garantir la maîtrise des informations figurant sur leur carte devait s'accompagner du droit d'en connaître le contenu entier, à charge pour le médecin qui donnerait ainsi accès à la carte, de donner toutes les explications nécessaires.

Plus récemment la Commission, lors de l'avis rendu sur le projet de disposition législative instituant le volet de santé de la future carte Vitale 2 [18], a considéré que l'usager devait avoir le droit de consulter, sans restriction, l'intégralité du contenu de ce volet, mais que des précautions devaient être prises s'agissant de la délivrance d'une copie papier de celui-ci, et ce pour éviter que des tiers (employeurs, compagnies d'assurance...) ne soient tentés par ce biais de faire pression sur l'usager pour obtenir communication d'informations médicales.

[18] Délibération du 18 février 1999. 20e rapport d'activités.

S'agissant de l'accès au dossier médical sur Internet, il semble nécessaire de distinguer deux situations : la situation du dossier d'urgence USIS pour laquelle il est logique et même indispensable que l'usager en connaisse le contenu, vital pour lui. La seconde situation, celle d'un véritable dossier médical partageable entre plusieurs professionnels de santé, est plus délicate : à cet égard, l'arbitrage qu'ont tenté de réaliser les deux associations de réseaux ville-hôpital, entre la nécessité de reconnaître au malade un véritable droit de regard sur les professionnels de santé habilités à accéder à son dossier et le souci, en ne prévoyant pas au moins au stade de l'expérimentation, un accès direct par Internet à l'intégralité de son dossier, de ne pas lui révéler trop brutalement des informations sur son état de santé, constitue un compromis intéressant mais fragile car tenant à l'aptitude des médecins qui auront à assurer le suivi des malades et à renseigner le dossier électronique, à informer de façon effective et claire ceux-ci des modalités de constitution et de communication de leur dossier.

Sans doute est-il difficile aujourd'hui de trancher brutalement en faveur d'un droit d'accès direct au dossier médical sur Internet et il sera intéressant à cet égard de disposer d'une évaluation des premiers mois de fonctionnement de ces projets. Mais, en tout état de cause, il semble clair qu'on ne peut à la fois donner à l'usager le pouvoir de décider de la création de son dossier de santé électronique, des autorisations d'accès à celui-ci et ne pas lui permettre d'y accéder lui-même.

C'est la raison pour laquelle la Commission, lors de l'examen des projets[19] , a estimé que l'usager auquel serait proposé un service de dossier de santé en ligne devait se voir remettre un document :

— précisant les modalités prévues de constitution, de mise à jour et d'accès au dos sier ainsi que les conséquences de l'utilisation, par les professionnels de santé, dudit dossier ;

— détaillant les conditions dans lesquelles il pourra lui-même accéder directement aux informations contenues dans ce dossier et éventuellement, les cas où il devra s'adresser à un médecin pour obtenir communication de certaines des informations contenues dans ce dossier

— indiquant l'identité de la société appelée à héberger les dossiers et les engage ments de confidentialité pris par cette dernière.

L'usager, ainsi informé, devra donner expressément son consentement à la constitution de son dossier, ce consentement devant pouvoir être modifié et retiré à tout moment.

2) LES CONDITIONS D'ACCES ET DE VALIDATION DES INFORMATIONS PAR LES PROFESSIONNELS DE SANTÉ

Les quatre projets prévoient que les informations conservées dans les dos-siers de santé accessibles sur Internet fassent l'objet d'une validation par des profes-

[19] Cf notamment délibérations du 8 mars 2001.

sionnels de santé, selon toutefois des modalités d'identification et d'authentification différentes.

En effet, pour que de tels dispositifs de dossiers de santé électroniques soient valides, les professionnels de santé comme les patients doivent pouvoir être assurés que les informations portées sur les dossiers de santé ont bien été saisies par des professionnels de santé dont l'identité et la qualité auront été certifiées, et qu'en cas de difficultés et de mise en cause de la responsabilité médicale, l'auteur de l'information erronée pourra ainsi être déterminé, ce qui suppose également qu'il soit gardé trace des créations et mises à jour des informations.

Dans la mesure où l'article 1316-1 du code civil (issu de la loi du 13 mars 2000) admet désormais l'écrit électronique au même titre que l'écrit sur support papier, les responsabilités qui pèsent sur le médecin ayant saisi ou validé un dossier de santé sur Internet semblent les mêmes que celles encourues lors de la rédaction d'un compte-rendu d'hospitalisation ou de l'établissement d'un certificat médical sur support papier. Ceci suppose cependant que les procédures de signatures électroniques retenues aient été considérées comme valides. La carte CPS du professionnel de santé, actuellement diffusée auprès des professionnels de santé libéraux dans le cadre du dispositif SESAM VITALE, s'est vue reconnaître par les textes des fonctions d'identification, d'authentification et de signature électronique. Néanmoins, cette carte n'est pas encore distribuée à l'ensemble des professionnels de santé. C'est la raison pour laquelle les responsables des quatre projets concernés ont été contraints d'envisager des solutions alternatives d'identification des professionnels de santé.

Pour la CNIL, la participation des professionnels de santé à la gestion sur Internet des dossiers médicaux de leurs patients doit s'accompagner d'une définition précise, par voie contractuelle, des conditions de leur adhésion et de leur responsabilité respective dans la gestion des dossiers médicaux sur Internet.

A cet égard, il importe donc que des systèmes d'identification et d'authentification sûrs des professionnels de santé soient mis en place pour garantir la validité des informations médicales appelées à figurer dans le dossier de santé électronique.

De façon corollaire, se pose la question de la durée de conservation des données portées sur les dossiers en ligne et du devenir de ceux-ci en cas d'arrêt de fonctionnement du réseau ou de non renouvellement de l'abonnement du professionnel de santé ou du patient. Sur ces points, les réponses demeurent incomplètes.

Les projets de réseau ville-hôpital, qui, de toutes façons, compte tenu de leur caractère expérimental, maintiendront la tenue d'un dossier médical papier, le dossier électronique « doublant » ce dernier, prévoient de conserver les dossiers de santé électroniques au moins pendant la durée de l'expérimentation et mentionnent la possibilité, dans le contrat qui lie le professionnel de santé à l'association concernée, de lui restituer une copie sous format électronique des informations « sur lesquelles il peut faire valoir des droits », c'est-à-dire des données qu'il aura lui-même fournies ou que le patient aura souhaité conserver.

Le projet présenté par la société Usis-Europe prévoit la possibilité de transférer le dossier de santé d'urgence d'un organisme à l'autre en cas de changement de

compagnie d'assurance par exemple. Mais, s'agissant de ce projet comme de celui d'Uni-Médecine, on peut légitimement se poser la question du devenir des données en cas d'abandon du dispositif : ne devraient-elles pas être restituées de façon systématique à l'usager ou au médecin désigné par ce dernier ?

C. L'intervention de sociétés commerciales dans le traitement du dossier de santé sur Internet

Les quatre projets ont pour caractéristique commune de faire appel aux services de sociétés commerciales pour assurer l'hébergement des dossiers de santé.

La Commission a déjà admis, sous certaines conditions, que des tiers non médecins puissent intervenir dans les traitements des données médicales, qu'il s'agisse de la maintenance des systèmes d'informations médicaux, notamment dans les hôpitaux, ou de l'intervention des organismes concentrateurs dans le cadre de la télétransmission des feuilles de soins électroniques.

Ainsi, le recours à un organisme tiers pour assurer le traitement technique des données de santé gérées sur Internet ne peut en effet être admis que, d'une part, si cet organisme s'engage à ne procéder à aucun traitement pour son propre compte ni à aucune cession ou mise à disposition des données à des tiers et d'autre part, si des dispositifs techniques, en particulier des moyens de chiffrement, sont mis en oeuvre pour garantir la confidentialité des données médicales.

1) L'INTERDICTION DE TOUTE UTILISATION COMMERCIALE DES DONNÉES

L'intervention de sociétés commerciales dans la gestion des systèmes d'informations de santé appelle une vigilance particulière dans la mesure où l'exploitation et la cession commerciale, sous une forme individuelle ou statistique, des données qu'elles sont appelées à traiter, peuvent constituer, pour ces sociétés, une source potentielle de financement.

En effet, il apparaît qu'à l'égal du constat fait sur les sites santé, le « business model » des projets de dossier médical sur Internet n'est pas aujourd'hui clairement défini, ce qui n'est d'ailleurs pas anormal, s'agissant d'une activité encore balbutiante et dont on ne sait si elle correspond aujourd'hui à une réelle attente, en France, du public et des médecins. Dès lors, il n'est pas illégitime de s'interroger sur les modalités selon lesquelles ces sociétés vont pouvoir rentabiliser leurs investissements.

La CNIL a certes pris acte de l'engagement pris par les sociétés de ne pas exploiter les données à des fins commerciales mais a souhaité réaffirmer le principe énoncé lors de sa recommandation précitée du 4 février 1997, selon lequel les données personnelles de santé ne peuvent être utilisées que dans l'intérêt direct du patient et dans des conditions déterminées par la loi, pour les besoins de la santé publique. Au delà, la CNIL a également considéré que l'activité de ces organismes

(infomédiaires) devrait faire l'objet d'un encadrement juridique et qu'il y avait lieu de prévoir des procédures d'agrément.

2) LES SECURITES

Tous les dispositifs de sécurité décrits dans les dossiers présentés à la CNIL reposent sur des mesures strictes d'accès physique et logique au serveur (firewall, codes utilisateurs, mots de passe).

L'ensemble des données appelées à circuler sur Internet feront l'objet, dans tous les projets, d'un chiffrement à 128 bits. Le déchiffrement des données ne pourra être effectué que par les utilisateurs disposant de droits d'accès aux données, la base des dossiers médicaux telle qu'hébergée chez la société prestataire faisant elle-même l'objet d'un chiffrement, ce à l'exception de la société Uni-Médecine où il serait envisagé que cette société puisse accéder en clair aux données. La CNIL a donc appelé l'attention de cette société sur ce point.

Délibération n° 01-012 du 8 mars 2001 portant avis sur un projet de décision présenté par l'Association pour la bonne coordination médico-chirurgicale concernant la mise en place d'un réseau ville-hôpital destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients bénéficiant d'une prise en charge médico-chirurgicale

La Commission nationale de l'informatique et des libertés ; Saisie pour avis du projet de décision présenté par l'Association pour la bonne coordination médico-chirurgicale ;

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

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

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

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

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

Formule les observations suivantes

L'Association pour la bonne coordination médico-chirurgicale (ABCMC) qui a pour objet la prise en charge médico-chirurgicale de patients adultes a saisi la Commission d'une demande d'avis ayant pour finalité l'expérimentation dans le cadre d'un réseau ville-hôpital d'un dossier de santé électronique sécurisé (« coffre fort électronique ») accessible sur Internet.

Participent au réseau les médecins des services de radiologie, de biophysique, de biologie et les services cliniques participant à la prise en charge médico-chirurgicale des patients ainsi que les médecins libéraux qui le souhaitent et qui auront adhéré à cette association.

Le dossier de santé électronique sera constitué et alimenté par les médecins assurant le suivi des patients et comportera les observations, prescriptions, résultats d'examens, diagnostics et traitements mais également des radiographies, scanners, échographies, IRM.

Sur les conditions de constitution et d'accès, par les usagers, au dossier de santé électronique

La Commission prend acte de ce que l'accord exprès de l'usager sera recueilli pour autoriser la création du dossier de santé électronique et que son consentement sera effectivement requis pour autoriser l'accès de ses données à d'autres professionnels de santé. La Commission estime que le professionnel de santé devra être averti, par un message spécifique, de la nécessité de recueillir le consentement de la personne lors de la communication à d'autres professionnels de santé de données du dossier de santé.

La Commission observe que le patient pourra accéder directement par Internet à certaines parties de son dossier médical et en particulier à sa fiche signalétique qui comporte son identité, son adresse, des données d'alerte médicales, l'identité des médecins traitants et un aide-mémoire personnel que lui seul peut visualiser. Le dossier de santé comporte également une fiche de liaison retraçant certains événements médicaux dont l'accès ne lui serait reconnu qu'après accord du professionnel de santé auteur de l'information. La Commission considère à cet égard que la possibilité désormais ouverte à chacun de pouvoir accéder en temps réel sur Internet à son dossier de santé devrait s'accompagner d'une maîtrise plus large des informations médicales appelées à figurer sur son dossier.

Elle estime que le document qui sera remis à l'usager lors de la création du dossier de santé électronique devra indiquer clairement les modalités prévues de constitution, de mise à jour et d'accès au dossier ainsi que les conséquences de l'utilisation, par les professionnels de santé, dudit dossier, les conditions dans lesquelles l'usager pourra lui-même accéder directement aux informations contenues dans ce dossier et, éventuellement, les cas où il devra s'adresser à un médecin pour obtenir communication de certaines des informations contenues dans ce dossier et enfin, l'identité de la société appelée à héberger les dossiers ainsi que les engagements de confidentialité pris par celle-ci.

La Commission considère que la remise de ce document doit être préalable au recueil du consentement exprès de l'usager pour la constitution de son dossier de santé, ce consentement pouvant être retiré et/ou modifié à tout moment.

Sur les conditions d'accès et de validation des informations par les professionnels de santé

La Commission observe que, dans le cadre de la phase expérimentale du projet, les accès des professionnels de santé seront assurés par des procédures de codes d'accès et de mots de passe attribués par le médecin désigné comme administrateur fonctionnel du réseau après que l'identité et la qualité

des médecins aient été vérifiées auprès du Conseil de l'ordre ; qu'à terme, l'identification, l'authentification ainsi que la signature électronique du professionnel de santé seront assurées par la carte de professionnel de santé.

La Commission estime que le recours à ce procédé permet d'assurer effectivement l'identification et l'authentification du professionnel de santé ; que chaque professionnel de santé participant au réseau devra en être doté dans les délais les plus rapides ; qu'à défaut, il conviendra que dans un délai de six mois à compter de la publication du décret d'application de la loi du 13 août 2000, un procédé de signature électronique soit mis en place. La Commission estime, en outre, que la participation des professionnels de santé au réseau devra s'accompagner d'une définition précise, par voie contractuelle, des conditions de leur adhésion et de leur responsabilité respectives dans la gestion sur Internet des dossiers médicaux de leurs patients.

Sur l'intervention de sociétés commerciales dans le traitement du dossier de santé sur Internet

Le projet prévoit que l'exploitation du serveur hébergeant les dossiers de santé électroniques est assuré en France par la société Accenture.

La Commission estime que l'intervention de sociétés commerciales dans la gestion des systèmes d'informations de santé appelle une vigilance particulière et qu'elle doit s'entourer de garanties appropriées de nature à éviter en particulier toute utilisation des données à des fins autres que celles pour lesquelles elles ont été collectées ainsi que toute cession à des tiers. •

A cet égard, la Commission prend acte des dispositifs de sécurité retenus pour assurer la sécurité physique et logique des dossiers de santé. Les informations appelées à circuler sur le réseau Internet feront l'objet d'un chiffrement à 128 bits suivant le protocole SHL et le déchiffrement des données ne pourra être effectué que par les professionnels de santé disposant de droits d'accès aux données.

La Commission prend également acte de l'engagement de la société Accenture de ne pas exploiter les données à des fins commerciales et de ne pas les céder à des tiers.

Compte tenu de ses observations la CNIL émet un avis favorable pour une durée de trois ans au projet d'acte réglementaire présenté par l'Association pour la bonne coordination médico-chirurgicale concernant la mise en place, à titre expérimental, d'un réseau ville-hôpital destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients et demande à être saisie d'un bilan de fonctionnement du réseau.

Délibération n° 01-013 du 8 mars 2001 portant avis sur un projet de décision présenté par l'Association Intégrale Santé concernant la mise en place d'un réseau de soins dans la région de Lens destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis du projet de décision présenté par l'Association Intégrale Santé de Lens ;

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

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

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

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

Vu l'arrêté du 1er août 2000 portant agrément d'une action expérimentale en application de l'article L 162-31-1 du code de la sécurité sociale ;

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

Formule les observations suivantes

L'Association Intégrale Santé regroupe les professionnels de santé de Lens qui ont crée le « réseau global d'exercice du bassin de vie de Lens et sa région », réseau agrée par le Comité d'orientation des filières et des réseaux de soins tel que prévu par l'article L 162-31-1 du code de la sécurité sociale. Cette association a saisi la CNIL d'une demande d'avis ayant pour finalité la mise en place à titre expérimental d'un dossier de santé électronique accessible sur Internet aux patients et aux différents acteurs impliqués dans le réseau et ce pour assurer une meilleure coordination des soins entre les professionnels de santé libéraux volontaires, le centre hospitalier de Lens et la caisse primaire d'assurance maladie de Lens. La population concernée serait constituée des assurés ou ayants-droit relevant du régime général résidant dans l'agglomération de Lens ainsi que dans les communes d'Avion, Méricourt, Rouvroy et Drocourt.

Le dossier de santé électronique sera constitué et alimenté par les médecins assurant le suivi des patients et comportera les observations, prescriptions, résultats d'examens, diagnostics et traitements mais également des radiographies, scanners, échographies, IRM.

Sur les conditions de constitution et d'accès, par les usagers, au dossier de santé électronique

La Commission prend acte de ce que l'accord exprès de l'usager sera recueilli pour autoriser la création du dossier de santé électronique et que son consentement sera effectivement requis pour autoriser l'accès de ses données à d'autres professionnels de santé. La Commission estime que le professionnel de santé devra être averti, par un message spécifique, de la nécessité de recueillir le consentement de la personne lors de la communication à d'autres professionnels de santé de données du dossier de santé.

La Commission observe que le patient pourra accéder directement par Internet à certaines parties de son dossier médical et en particulier à sa fiche signalétique qui comporte son identité, son adresse, des données d'alerte médicales, l'identité des médecins traitants et un aide-mémoire personnel que lui seul peut visualiser. Le dossier de santé comporte également une fiche de liaison retraçant certains événements médicaux dont l'accès ne lui

serait reconnu qu'après accord du professionnel de santé auteur de l'information.

La Commission considère à cet égard que la possibilité désormais ouverte à chacun de pouvoir accéder en temps réel sur Internet à son dossier de santé devrait s'accompagner d'une maîtrise plus large des informations médicales appelées à figurer sur son dossier.

Elle estime que le document présenté sous forme de charte qui sera remis à l'usager lors de la création du dossier de santé électronique devra indiquer clairement les modalités prévues de constitution, de mise à jour et d'accès au dossier ainsi que les conséquences de l'utilisation, par les professionnels de santé, dudit dossier, les conditions dans lesquelles l'usager pourra lui-même accéder directement aux informations contenues dans ce dossier et, éventuellement, les cas où il devra s'adresser à un médecin pour obtenir communication de certaines des informations contenues dans ce dossier et enfin, l'identité de la société appelée à héberger les dossiers ainsi que les engagements de confidentialité pris par celle-ci.

La Commission considère que la remise de ce document doit être préalable au recueil du consentement exprès de l'usager pour la constitution de son dossier de santé, ce consentement pouvant être retiré et ou modifié à tout moment.

Sur les conditions d'accès et de validation des informations par les professionnels de santé

La Commission observe que, dans le cadre de la phase expérimentale du projet, les accès des professionnels de santé seront assurés par des procédures de codes d'accès et de mots de passe attribués par le médecin désigné comme administrateur fonctionnel du réseau après que l'identité et la qualité des médecins aient été vérifiées auprès du Conseil de l'ordre ; qu'à terme, l'identification, l'authentification ainsi que la signature électronique du professionnel de santé seront assurées par la carte de professionnel de santé.

La Commission estime que le recours à ce procédé permet d'assurer effectivement l'identification et l'authentification du professionnel de santé ; que chaque professionnel de santé participant au réseau devra en être doté dans les délais les plus rapides ; qu'à défaut, il conviendra que dans un délai de six mois à compter de la publication du décret d'application de la loi du 13 août 2000, un procédé de signature électronique soit mis en place.

La Commission estime, en outre, que la participation des professionnels de santé au réseau devra s'accompagner d'une définition précise, par voie contractuelle, des conditions de leur adhésion et de leur responsabilité respectives dans la gestion sur Internet des dossiers médicaux de leurs patients.

Sur l'intervention de sociétés commerciales dans le traitement du dossier de santé sur Internet

Le projet prévoit que l'exploitation du serveur hébergeant les dossiers de santé électroniques est assuré en France par la société Accenture.

La Commission estime que l'intervention de sociétés commerciales dans la gestion des systèmes d'informations de santé appelle une vigilance particulière et qu'elle doit s'entourer de garanties appropriées de nature à éviter en

particulier toute utilisation des données à des fins autres que celles pour lesquelles elles ont été collectées ainsi que toute cession à des tiers.

A cet égard, la Commission prend acte des dispositifs de sécurité retenus pour assurer la sécurité physique et logique des dossiers de santé. Les informations appelées à circuler sur le réseau Internet feront l'objet d'un chiffrement à 128 bits suivant le protocole SHL et le déchiffrement des données ne pourra être effectué que par les professionnels de santé disposant de droits d'accès aux données.

La Commission prend également acte de l'engagement de la société Accenture de ne pas exploiter les données à des fins commerciales et de ne pas les céder à des tiers.

Compte tenu de ses observations la CNIL émet un avis favorable pour une durée de trois ans au projet d'acte réglementaire présenté par l'Association Intégrale Santé de Lens concernant la mise en place, à titre expérimental, d'un réseau de soins dans la région de Lens destiné à permettre la gestion et l'archivage sur Internet des dossiers de patients et demande à être saisie d'un bilan de fonctionnement du réseau.

Chapitre 7

CRÉDIT ET PAIEMENT :

LA SÉCURITÉ « TOUT PRIX ?

I. LA SECURISATION DES CARTES BANCAIRES

Une polémique assez confuse sur la sécurisation de la carte bancaire et les risques de décryptage des protections informatiques installées sur cette carte a conduit le gouvernement à engager une réflexion sur la sécurisation des paiements à distance.

Ainsi, en avril 2000, le secrétariat d'État aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation a décidé la création d'un groupe de travail sur la sécurité des cartes bancaires. La CNIL a été invitée à participer aux réunions rassemblant les associations de consommateurs, les différents acteurs économiques du secteur représentant la distribution et le commerce, les établissements de crédit, les industriels de la monétique, le groupement des cartes bancaires, ainsi que les différentes entités publiques concernées.

La mission de ce groupe de travail était de faire le point sur les différents types de fraude aux cartes de paiement, de formuler des recommandations visant à limiter la fraude et d'exercer le suivi des mesures annoncées par le groupement des cartes bancaires, notamment en matière de suppression du numéro complet de la carte figurant sur les facturettes.

La CNIL est à l'origine de cette mesure réclamée par les pouvoirs publics.

Sensibilisée à cette question au travers des plaintes qu'elle reçoit régulièrement sur ce sujet, la Commission avait demandé au groupement des cartes bancaires, à la suite d'une visite qui s'est déroulée en mai 1999, de prendre des mesures en la matière. Les particuliers qui saisissent la CNIL s'étonnaient que les tickets édités

par les terminaux de paiement électronique puissent comporter l'indication de leur nom et prénom, ainsi que le numéro et la date d'expiration de la carte bancaire. Ces plaignants faisaient part de l'inquiétude que ces informations puissent être utilisées pour réaliser des paiements à distance, ce qui augmente considérablement les risques de fraude en cas de perte du ticket. Les exemples de fraudes révélées par des plaintes déposées auprès de la CNIL confirment d'ailleurs que cette inquiétude est fondée et les travaux menés par le groupe de travail l'ont largement prouvé. La Commission a fait valoir au groupement des cartes bancaires que seule une réponse technique, au niveau des terminaux électroniques de paiement, pourrait permettre de remédier à cette situation.

En janvier 2000, le groupement des cartes bancaires décidait d'introduire dans le cahier des charges permettant aux industriels de développer leurs logiciels la suppression de l'impression du nom et l'obligation de tronquer le numéro de carte et sa date d'expiration sur les tickets de paiement remis au client lors d'un achat. Cette disposition est une condition d'agrément « CB » des terminaux.

Il reste cependant à mettre en oeuvre de façon concrète cette mesure par une mise à jour de l'ensemble du parc des terminaux de paiement car, au premier trimestre 2001, il apparaissait que seuls 10 % des points de vente avaient été mis aux normes. Or, ce type de mesure a, depuis plusieurs années déjà, été mis en œuvre par les établissements financiers en ce qui concerne les distributeurs de billets.

Le groupement des cartes bancaires, le Conseil du commerce de France et Mercatel (émanation du Conseil du commerce spécialisée dans les nouvelles technologies) ont décidé la création d'un groupe de travail chargé d'assurer le suivi et la mise en œuvre de cette recommandation avant la fin de l'année 2001.

La polémique s'est focalisée sur le paiement sur Internet alors que les numéros de carte représentent un facteur important de fraude dans le cadre de la vente à distance, tous vecteurs confondus, qu'il s'agisse du téléphone, du Minitel et pas spécifiquement d'Internet.

Parmi les recommandations du groupe du travail concernant les établissements de crédit et les émetteurs de cartes, il est préconisé de mieux informer les utilisateurs et, notamment, le porteur de la carte du montant de son plafond d'autorisation. La CNIL avait déjà, il y a plusieurs années, alerté l'Association Française des Banques et l'Association des Sociétés financières sur cette question et certains réseaux bancaires avaient mis en place des procédures d'information claires pour leurs clients, qui vont ainsi être généralisées à l'ensemble de la profession.

Afin de sécuriser les achats à distance, le rapport du CNC évoquait la mise en place de fichiers d'incidents au niveau professionnel mais ce point n'a pas été repris par la charte signée en février 2001 par les professionnels. Il convient de préciser que la Commission est favorable en la matière à un encadrement législatif précis concernant les conditions d'inscription, la durée de conservation et les droits des personnes.

Une autre crainte est souvent exprimée par les personnes qui saisissent la Commission. Il s'agit du risque de captation du numéro de carte bancaire lorsqu'il

transite sur Internet. Sur ce point, la Commission croit devoir rappeler que dès lors que l'on n'a pas à taper son code secret, des fraudes sont possibles et que les solutions qui reposent sur des mécanismes d'authentification des acheteurs sont les plus fiables, que le risque de captation du numéro de carte n'est pas plus grand sur Internet que lorsque ce numéro est communiqué par Minitel ou téléphone — il est d'ailleurs moindre dans la mesure où, comme l'atteste l'étude de la CNIL sur cent principaux sites de commerce électronique français, le numéro de carte bancaire est sécurisé, c'est-à-dire chiffré, dans 96 % des cas (Cf. 20e rapport d'activité 1999, p. 101).

En revanche, les risques d'intrusion dans les fichiers des commerçants disposant des références bancaires sont réels et augmentent avec le nombre de sites de commerce électronique. C'est pourquoi la Commission juge essentiel que les mesures de sécurité concernent ces fichiers eux-même tout autant que le réseau. De plus, la Commission rappelle que la conservation du numéro de carte bancaire dans un traitement automatisé d'informations nominatives doit en premier lieu s'effectuer dans le respect des dispositions posées par l'article 5 de la convention n° 108 du Conseil de l'Europe, c'est-à-dire pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles l'information est exigée. En l'espèce, cette donnée doit permettre de réaliser une transaction. Sa durée de conservation ne peut donc être que très limitée. Par ailleurs, le numéro de carte bancaire ne saurait devenir ni un identifiant de la clientèle ni une donnée de type marketing. De tels usages pourraient notamment nuire à la sécurité des informations en facilitant la diffusion du numéro à des tiers non autorisés et, ainsi, les pratiques frauduleuses.

Le rapport du Conseil national de la consommation reprend ces recommandations de la CNIL à l'attention du secteur de la vente à distance en préconisant aux commerçants « de ne pas stocker dans des bases de données des informations relatives aux numéros de cartes et de cryptogrammes visuels ».

La Commission avait également attiré l'attention du groupement des cartes bancaires en 1999 sur la nécessité de veiller au respect de la finalité du paiement ayant présidé à la collecte des informations relatives à la carte bancaire. Le groupement des cartes bancaires avait indiqué en réponse qu'afin d'éviter que les commerçants stockent et utilisent les données à d'autres fins que celles du paiement, une disposition spécifique du contrat d'acceptation en télépaiement sécurisé oblige le commerçant en ligne à respecter la finalité du paiement.

Les représentants des secteurs bancaires et du commerce ont signé le 22 février 2001 une charte qui reprend les recommandations précitées du rapport du CNC. Par ailleurs, un projet de loi relatif à la sécurité quotidienne doit également permettre d'améliorer la sécurité des cartes de paiement tant sur le plan préventif (la Banque de France devra s'assurer de la sécurité des moyens de paiement) que sur le plan répressif (le projet instaure une nouvelle infraction pénale qui consiste à incriminer le fait de fabriquer, d'acquérir, de détenir ou de mettre à disposition des équipements, instruments, programmes ou données adaptés pour falsifier ou contrefaire des cartes bancaires).

II. L'EMBLEMATIQUE SECTEUR DU CREDIT

Le secteur du crédit est un secteur économique déterminant puisqu'il contribue à dynamiser la consommation des ménages. C est également un secteur sensible dans la mesure où, en profonde mutation, il s'ouvre désormais à la concurrence européenne ou étrangère.

Au regard des missions de la CNIL, il s'avère propice à la prolifération des traitements d'informations, qu'il s'agisse de gérer les crédits accordés, d'évaluer la capacité de remboursement des candidats au crédit ou de prévenir les fraudes.

Enfin, au regard de la vie privée des personnes, il est peu d'occasions où l'on se voit demander autant de renseignements que lorsque l'on sollicite un prêt. Aussi ce domaine d'activités est-il un de ceux qui, depuis des années, suscite le plus grand nombre de plaintes de particuliers auprès de la CNIL.

L'ensemble de ces raisons ont conduit le législateur mais aussi la CNIL à intervenir dans ce domaine. ◦ ce titre, il convient de rappeler que la loi n° 89-1010 du 31 décembre 1989 relative à la prévention et au règlement judiciaire des difficultés liées au surendettement des particuliers et des familles a confié à la Banque de France la gestion d'un fichier recensant les incidents de paiement (FICP), sur la mise en œuvre duquel la CNIL a, à plusieurs reprises, donné son avis.

La CNIL a par ailleurs adopté, par délibération n° 88-83 du 5 juillet 1988, une recommandation sur la gestion des crédits ou des prêts consentis à des personnes physiques par des établissements de crédit. Cette recommandation a été complétée par une délibération n° 98-101 du 22 décembre 1998 portant sur l'utilisation de la nationalité comme variable d'appréciation du risque d'impayé. Cette dernière délibération a fait l'objet d'un recours pour excès de pouvoir qui est à ce jour pendant devant le Conseil d'État.

Les professionnels ont fait valoir que la fraude à l'obtention de crédit, si elle n'est pas un phénomène nouveau, tendrait à se développer et à s'organiser.

Au-delà de la part de la fraude individuelle, qui relève essentiellement de l'astuce ou de la tricherie — le client cherchant à présenter sa situation sous le meilleur jour possible, il y aurait désormais une fraude beaucoup plus organisée, structurée en réseaux et relevant d'un comportement mafieux. Cette fraude au crédit incite naturellement les professionnels à mieux s'organiser.

Ce sont ces modalités d'organisation, dont toutes ne sont pas cependant nouvelles, qui ont déterminé la CNIL à procéder à des vérifications sur place auprès de plusieurs établissements représentant près de 60 % du marché du crédit à la consommation.

A. Les précédents

La Commission a été saisie des premiers dossiers de déclaration relatifs à la constitution de « fichiers de protection » dès 1994 (cf. rapport d'activité 1994 p. 134).

Plusieurs préconisations ont alors été dégagées :
les traitements liés à la lutte contre la fraude doivent demeurer de la seule compétence d'un service centralisé et spécialisé, chargé dans les cas de suspicion de fraude de procéder à des vérifications approfondies ; seuls les membres de ce service, qui doivent disposer d'un mot de passe personnel, sont habilités à traiter les informations et à procéder aux analyses nécessaires, cela en dehors de tout automatisme,
les services d'exploitation en relation avec la clientèle doivent soumettre les dossiers semblant présenter des irrégularités à l'appréciation du service central,
une anomalie avérée entraîne, dans le fichier centralisé de la clientèle de l'établissement, l'enregistrement d'un code signifiant que toute nouvelle demande devra lui être transmise ; le signalement des dossiers doit disparaître dès lors que les vérifications ont levé les doutes,
les intéressés doivent être informés sur le formulaire de demande de crédit que toute déclaration irrégulière peut faire l'objet d'un traitement spécifique à l'égard duquel ils disposent d'un droit d'accès et de rectification.

Par la suite, les autres établissements qui souhaitaient mettre en place un système de lutte contre la fraude se sont alignés sur ces recommandations.

B. Le constat des missions de vérification sur place

La délégation de la Commission a pu constater que les modalités de fonctionnement des fichiers de protection interne, fixées en 1994, sont respectées.

Les établissements ont bien mis en place des services ou cellules, spécialisés et centraux, composés au maximum d'une dizaine de personnes détachées de la gestion de la clientèle. Des systèmes de sécurité protègent l'accès physique à ces cellules. Les applications de « lutte contre la fraude » fonctionnent sur des matériels informatiques dédiés. Elles sont isolées des autres fichiers détenus par l'établissement, tel que le fichier des impayés ou le fichier clientèle, et protégées par des mots de passe. Les seules passerelles existantes entre ces différents traitements sont en fait les codes d'alerte émis depuis la cellule de lutte contre la fraude. Par essence, ces derniers apparaissent dans l'application clientèle afin de signaler aux agents commerciaux que le dossier doit être envoyé pour une étude plus approfondie à la cellule spécialisée.

L'enregistrement de données dans les fichiers fraude s'opère au niveau central. Il repose toujours sur des éléments concrets : les dossiers papiers sont conservés comme support de preuve. Ainsi, une inscription liée à la falsification d'un bulletin de salaire ne peut être réalisée que si le service dispose concrètement du faux bulletin.

Les établissements contrôlés ont soit affirmé ne pas conserver plus de 5 ans les données dans leur fichier de protection interne, grâce par exemple à la programmation de l'opération d'effacement, soit indiqué que leur traitement fonctionnait depuis moins de 5 ans. L'un d'entre eux a toutefois précisé que pour les fraudes légères (majoration du salaire réel, fausses attestations de domicile...), la durée de conservation était fréquemment ramenée à 3 ans.

Dès lors que les personnes sont préalablement informées d'une telle identification et que le fichier demeure à usage purement interne, de telles pratiques ne paraissent pas contraires à la loi « informatique et libertés ». Sans doute convient-il de veiller à ce que la durée de conservation d'une telle identification ne soit pas illimitée, pour faire sa part au « droit à l'oubli », et harmonisée.

En tout état de cause, toutes les personnes doivent pouvoir exercer leur droit d'accès et avoir, à cette occasion, connaissance de cette identification ainsi que de sa signification concrète. Enfin, l'article 26 de la loi du 6 janvier 1978 leur permet d'invoquer, le cas échéant, des raisons légitimes pour s'opposer à une telle identification, le juge judiciaire étant, en dernière instance, seul compétent pour apprécier la légitimité d'une telle demande d'effacement.

Il existe cependant un partage du savoir-faire en matière de lutte contre la fraude. En effet, les établissements qui ont déclaré des fichiers de protection, en nombre assez limité, assurent bien souvent la gestion des crédits d'autres établissements, banques ou commerçants. Dans ce cadre, leurs agents sont amenés à instruire des dossiers qui ont été constitués à l'origine pour d'autres enseignes que la leur. Or, l'instruction du dossier aboutira à un contrôle de cohérence susceptible, en cas de doute, de déboucher sur le renvoi des pièces vers la cellule de lutte contre la fraude. Au final, celle-ci ne traitera donc pas uniquement des demandes de crédit déposées auprès de l'établissement dont elle dépend directement — et qui est pour la CNIL le responsable d'un fichier « fraude » — mais aussi toutes les suspicions en provenance de ses partenaires.

Cela signifie, en pratique, que le fichier « fraude » d'un établissement A va comporter des données collectées à l'occasion de demandes déposées auprès des établissements B, C, D, etc., dont il assure la gestion des crédits.

Cette pratique apparaît tout à fait naturelle aux établissements, dans la mesure où ils sont effectivement en charge, c'est-à-dire responsables, du traitement des dossiers de crédit pour d'autres sociétés. Au niveau des fichiers de protection, cette pratique peut se traduire par l'existence d'un code spécifique par société d'appartenance du client et/ou d'une mention écrite sur le dossier papier.

Cependant, pour le client, le système est tout à fait opaque puisqu'il n'est à aucun moment informé que toute demande irrégulière pourra faire l'objet d'un traitement spécifique par la société X. Ce faisant, il ne pourra en aucun cas exercer son droit d'accès et de rectification ni un éventuel droit d'opposition pour des raisons légitimes. Des explicitations précises sont, donc, nécessaires à l'avenir.

C. Les demandes de renseignements auprès de tiers

Les professionnels interrogent fréquemment les mairies et les employeurs afin d'obtenir des renseignements. Il s'agit là d'une pratique courante pour laquelle certains établissements recourent à des courriers types. De telles pratiques sont évidemment légitimes lorsqu'elles se bornent à vérifier auprès de tiers la véracité des informations qui ont été collectées auprès des candidats au crédit. Cependant, la délégation de la CNIL a pu constater que de nombreux courriers vont au-delà de ces simples demandes de vérification et sont utilisés pour collecter de nouvelles données à l'insu des personnes concernées.

Ainsi, les courriers types d'un même établissement, l'un adressé aux employeurs, l'autre aux mairies, visaient à recueillir, outre la nouvelle adresse, des informations sur les parents du client.

Un autre établissement a indiqué avoir renoncé, à la suite d'un différend avec un client, à faire figurer dans ses demandes écrites une question relative aux saisies sur salaire.

La CNIL est quelquefois saisie de plaintes sur ce point. Ainsi, un travailleur frontalier s'est étonné auprès d'elle de ce que l'un de ses créanciers avait adressé à son employeur une lettre dans laquelle il lui était demandé si une saisie sur salaire était intervenue et, le cas échéant, quels étaient la quotité saisie et les organismes créanciers.

De telles pratiques, lorsqu'elles ont pour objet non plus de vérifier la véracité d'éléments déclarés mais de recueillir de nouveaux renseignements à l'insu des personnes concernées, sont à proscrire et, en tout état de cause, contraires aux dispositions de l'article 25 de la loi du 6 janvier 1978.

Les établissement peuvent également avoir des contacts avec les services de police par le biais de réquisitions judiciaires qui leur sont adressées. Au regard de la loi « informatique et libertés », ces contacts ne soulèvent pas de difficultés dans la mesure où la police constitue un tiers autorisé à avoir accès aux informations contenues dans un fichier dès lors que ces informations peuvent intéresser une affaire judiciaire. Cependant, les établissements interrogés par la police peuvent être tentés de conserver trace des informations qui leur auront été fournies dans le cadre de ces réquisitions (l'identité d'un escroc présumé, par exemple), même lorsque la personne concernée dont l'identité est ainsi révélée n'est pas un client de cet établissement. Ainsi, un des établissements contrôlés a manifesté son souhait de pouvoir procéder à l'enrichissement de son fichier de protection contre la fraude à partir des identités des personnes recherchées et transmises par la police, que ces dernières soient ou non clientes.

De telles pratiques, qui aboutissent à la prolifération de « listes noires » sans aucune garantie, sont à proscrire au regard de la loi « informatique et libertés » comme excédant la finalité des traitements et méconnaissant les droits des personnes concernées.

D. Le risque d'automatisation de profils de fraudeurs ou « l'ilôtypage négatif »

Les systèmes d'information géographique consistent, à partir du recoupement d'informations, à caractériser non pas le « profil » d'une personne, mais celui d'un territoire (l'ilôt) dont les caractéristiques seront supposées être celles du groupe, considéré comme homogène, de ses habitants. L'ilôt, unité statistique de base, correspond à un « pâté de maisons » ou à une zone de peuplement considérée comme homogène et comportant en moyenne 150 habitants.

L'ilôtypage est utilisé de manière courante à des fins de prospection commerciale. Il s'agit alors, par le maillage du territoire, de limiter la prospection commerciale aux seuls zones géographiques ou quartiers supposés correspondre à la « cible commerciale » du produit. De telles pratiques, au demeurant courantes, n'appellent aucune observation particulière. Il n'en est pas de même de « l'ilôtypage » dit négatif.

L'ilôtypage est dit « négatif » quand il ne s'agit plus de sélectionner une cible commerciale, mais d'exclure toutes les personnes d'un même ilôt considéré comme étant à risques.

Rapporté au crédit, il s'agirait alors d'exclure du crédit ou de procéder systématiquement à des vérifications complémentaires en fonction de l'adresse (quartier, immeuble) du demandeur au crédit.

La CNIL a ainsi été saisie, en mars 2000, d'une déclaration déposée par un établissement de crédit qui évoquait une utilisation future de l'ilôtypage lors de l'examen préalable des demandes de crédit. Cette technique permettrait de déterminer la cohérence d'un dossier au regard des caractéristiques présentées par la population du pâté de maisons (îlot) qu'habite le demandeur, par exemple par comparaison entre le revenu déclaré et le revenu moyen de l'îlot. Si l'établissement déclarant a finalement indiqué ne recourir à la segmentation géographique qu'à des fins de marketing, il a aussi précisé se réserver le droit de l'utiliser à terme pour l'octroi de prêts ou la lutte contre la fraude, dans la mesure où cet outil est disponible sur le marché.

Il résulte des missions de contrôle menées qu'à l'heure actuelle les établissements n'utilisent pas les outils offerts par les systèmes d'information géographique dans le cadre de la lutte contre la fraude ou même de l'octroi des crédits. Lorsqu'elle n'est pas totalement absente, cette technique demeure limitée au secteur du marketing.

Cependant, une telle unanimité de principe ne doit pas dissimuler que, si elle trouve son explication dans des motifs déontologiques, le manque de pertinence de l'outil est également souvent invoqué. En effet, si les techniques de segmentation géographiques se sont révélées efficaces en Grande-Bretagne dans le secteur du crédit, elles apparaîtraient en revanche inadaptées au marché français. Les informations statistiques ne seraient pas assez précises : les îlots sont trop larges et ne permettent pas de déterminer des profils sociologiques suffisamment proches de la réalité pour être pertinents.

E. Le problème posé par la pratique des appels aux voisins

La CNIL est de plus en plus souvent saisie de réclamations, écrites ou téléphoniques, relatives à des contacts pris par les sociétés financières avec des proches, voisins, parents ou amis de clients en situation d'impayés.

Face aux échéances impayées et redoutant que le débiteur ne se dérobe, certains établissements n'hésitent pas à appeler des voisins qu'ils identifient, notamment, grâce à l'annuaire téléphonique.

Les services de lutte contre la fraude des établissements contrôlés ont indiqué ne pas rechercher ce type de contact. Mais ils travaillent tous en relation avec le service de recouvrement de créance.

Les contacts avec la famille ou les voisins sont toujours anonymes : les agents des établissements de crédit donnent leur identité, ainsi qu'un numéro de téléphone où ils peuvent être joints, mais ne précisent pas à quelle société ils appartiennent ni qu'il s'agit d'une créance à recouvrer. Ils espèrent qu'ainsi informés du type de méthode employée à leur égard, les débiteurs souhaiteront éviter qu'elles se prolongent...

À l'exception d'un établissement reconnaissant qu'il s'agissait d'une pratique courante pour ses services, les autres professionnels contrôlés ont indiqué ne recourir à de telles méthodes que de façon tout à fait exceptionnelle, afin de retrouver un client qui n'a pas préalablement répondu à des sollicitations écrites ou dont les coordonnées ont changé.

Si les contacts avec les tiers à des fins de recherche d'informations sur le débiteur sont possibles, ils sont étroitement encadrés par le loi et relèvent en dernier lieu du procureur de la République, saisi par l'huissier de justice. Cette mesure a été ainsi justifiée par le ministre de la Justice dans une réponse à la question écrite d'un parlementaire : « Le ministère public, et lui seul, peut obtenir auprès des établissements, organismes ou administrations concernés, à la demande de l'huissier de justice chargé de l'exécution, certaines informations confidentielles relatives au débiteur » (adresse, nom de l'employeur ou des établissements auprès desquels un compte est ouvert au nom du débiteur).

L'intervention de l'autorité judiciaire constitue en effet la garantie nécessaire permettant la levée du secret protégeant la liberté individuelle et la vie des personnes (Rép. min., min. de la Just., n° 23374 : JOAN Q, 6 octobre 1995, p. 4357.).

Un arrêt de la cour d'appel de Rennes du 29 octobre 1999 a par ailleurs condamné un établissement de crédit ayant recouru à de telles pratiques à verser à l'une de ses clientes en situation d'impayé des dommages-intérêts pour avoir porté atteinte à l'intimité et au secret de sa vie privée, d'une part en révélant à des tiers sa situation financière et, d'autre part, en ayant exercé de mauvaise foi des pressions sur ces tiers afin de les amener à agir sur la débitrice.

Les appels téléphoniques à des voisins ou des parents, dans le cadre de la gestion d'un crédit, constituent une pratique contraire à l'article 29 de la loi du 6 janvier 1978, sanctionnée pénalement par l'article 226-17 du nouveau code pénal.

La révélation à un voisin de la situation personnelle d'un débiteur fiché est évidemment contraire à ces dispositions. Certes, la plupart des établissements peuvent prétendre y échapper dès lors que l'appel aux voisins ne révélerait ni son objet ni sa provenance. En pratique, il suffit cependant qu'un voisin indélicat appelle le numéro de téléphone qui lui aura été laissé par l'établissement de crédit pour être communiqué au débiteur pour savoir de quoi il s'agit.

Cette pratique peut aussi, si elle donne lieu à l'enregistrement des coordonnées du voisin ou du parent dans le fichier, être contraire à l'article 25 de la loi en vertu duquel la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite. Enfin, sur un autre terrain que la protection des données personnelles, elle peut constituer une atteinte au secret professionnel auquel sont tenus les établissements de crédit, en vertu de la loi bancaire.

L'ASF a mis en place un processus de certification demandant à ses membres de respecter une « graduation » des démarches et une modération en matière de recouvrement amiable. Elle a également entamé des discussions sur ce point avec les associations de consommateurs. Un autre établissement financier a finalement, à la suite des démarches entreprises par la CNIL, fait savoir officiellement qu'il renonçait de manière absolue à de telles pratiques.

Sans doute ce débat mériterait-il encore, de la part des professionnels, réflexion et évolution.

F. La communication des informations collectées lors d'un crédit à d'autres sociétés

Il est très fréquent que les données nominatives recueillies dans le cadre d'une demande de crédit soient transmises à des partenaires commerciaux ou financiers, tels que des assureurs. Cette transmission est, en pratique et au moins formellement, autorisée par les clients eux-mêmes : les offres préalables de crédit ou les contrats incluent en effet généralement une clause prévoyant la levée du secret bancaire.

Cette clause est en pratique souvent couplée avec les mentions relatives à la loi « informatique et libertés » et les objectifs de la cession (prospection commerciale ou exécution du contrat) sont rarement précisés ou différenciés, ce qui rend tout à fait théorique l'exercice éventuel du droit d'opposition qui est formellement reconnu.

Il n'est souvent fait aucune distinction entre les destinataires également soumis au secret professionnel et les autres, tels que les partenaires commerciaux.

Dès lors, la situation demeure globalement très insatisfaisante au regard de l'obligation de transparence à l'égard des personnes posée par la loi de 1978.

En règle générale, hors disposition légale particulière, telle précisément celle protégeant par le secret bancaire les données détenues par les établissements de crédit, la loi du 6 janvier 1978 n'interdit pas les échanges ou les cessions de données à des partenaires ou à des sociétés tierces dès lors que les personnes en sont informées et ont été mises en mesure de s'y opposer. En outre, et de manière plus générale, les personnes doivent être clairement informées de la finalité du traitement et des destinataires des données. La directive européenne du 24 octobre 1995 renforce d'ailleurs ces garanties (articles 10, 11 et 14 de la directive).

C'est à ce titre que la Commission ne cesse de recommander que les mentions d'informations soient claires et lisibles et préconise l'apposition d'une case à cocher sur les questionnaires de collecte d'informations, de sorte que les personnes concernées puissent aisément exercer leurs droits. De nombreux professionnels ont trouvé avantage à respecter ces recommandations.

Certes, plus l'information est précise, plus les personnes concernées pourront exercer leurs droits et les professionnels redoutent sans doute qu'il résulte d'une bonne application de la loi une moindre possibilité pour eux de céder les données à des tiers. Ils peuvent même soutenir que, s'agissant de cessions limitées à un nom et une adresse, le préjudice résultant d'une information moins claire est marginal puisque la seule conséquence pour les personnes concernées serait de recevoir un document de prospection indésiré ou indésirable d'une société avec laquelle ils ne sont pas en contact.

G. L'application du secret bancaire

Lorsque le secret professionnel est en cause, sa levée par le client suppose un accord exprès.

Et la profession bancaire est soumise au secret professionnel garanti par l'article 226-13 du nouveau code pénal selon l'article *57* de la loi bancaire de 1984 :

Tout membre d'un conseil d'administration et, selon le cas, d'un conseil de surveillance et toute personne qui à un titre quelconque participe à la direction ou à la gestion d'un établissement de crédit ou qui est employé par celui-ci, est tenu au secret professionnel dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal.

Aucun texte ne précise cependant l'étendue du secret professionnel auquel est tenu l'établissement de crédit. Celui-ci peut communiquer à des tiers des renseignements très généraux sur la situation économique ou financière de ses clients en vertu de ce que l'on appelle « l'opinion de la place » (Cass. com., 5 février 1962). Cette pratique est considérée comme compatible avec le secret professionnel « si les indications données sont générales et peuvent s'appuyer sur des éléments connus sur la place ».

La jurisprudence en la matière est rare ; certains précédents incitent à une analyse au cas par cas tenant le plus grand compte des circonstances entourant la

transmission des données et les « règles en usage dans la profession » (CA Paris, 6 février 1975). Il est certain, en tout cas, que le banquier ne peut pas communiquer, sans violer le secret professionnel, « les informations confidentielles s'apparentant à des données précises, tels notamment des éléments chiffrés non légalement relevés (mouvements d'un compte, versements particuliers, solde...), (CA Rennes, 13 janvier 1992).

La Commission s'en tient aux orientations admises par le Comité de la Réglementation Bancaire sur le sujet : un établissement de crédit n'est pas habilité à transmettre à des tiers des données nominatives concernant sa clientèle, même lorsque ces tiers sont des sociétés qui lui sont liées par des liens de capital, sauf à ce que cette transmission prenne la forme de la fourniture de renseignements commerciaux d'ordre général, en réponse à une interrogation ponctuelle et conformément aux usages de la profession.

C'est notamment au regard de telles considérations que, selon la Commission, un fichier commun aux professionnels devrait faire l'objet d'un encadrement législatif (cf. *infra).*

H. La réflexion des professionnels sur l'éventuelle constitution d'un fichier commun de lutte contre la fraude

Il s'agirait de mettre en place un système centralisé fondé sur le caractère volontaire de l'adhésion des organismes de crédit qui recenserait les informations relatives aux fraudes les plus graves, telles que la production de faux documents, dans le but d'en organiser l'échange entre établissements de crédit. La durée de conservation de ces informations serait de 8 ans, par analogie avec la durée de conservation la plus longue retenue dans le cadre du FICP.

Il pourrait être soutenu que de tels fichiers communs existent dans d'autres secteurs qui mêlent impayés et comportements frauduleux. Tel est le cas notamment d'un fichier déclaré par le GIE Préventel en matière de téléphonie mobile.

La Commission a toujours veillé avec une attention particulière aux modalités entourant la création de fichiers centraux. En 1988, dans sa recommandation relative à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements de crédit, elle a ainsi prévu, pour les fichiers communs d'incidents de paiement :

que les personnes concernées doivent être informées dès la sollicitation du prêt que les données les concernant sont susceptibles d'être inscrites dans un fichier ac cessible à l'ensemble des professionnels du crédit, cet avertissement devant être re nouvelé avant l'inscription ou au moment où il y est procédé,

lorsqu'un établissement tient compte d'informations recensées dans un fichier central pour refuser un crédit, il doit communiquer au requérant la nature et l'origine de ces informations, de sorte que la personne soit mise en mesure d'y avoir accès et, le cas échéant, de les contester,

que toutes les précautions doivent être prises afin d'éviter les risques de confusion liés à des homonymies,

— que seuls les cas présentant un niveau grave d'impayés[20] doivent donner lieu à une inscription,
— qu'enfin, la durée de conservation ne doit pas en tout état de cause dépasser 3 ans pour les dossiers soldés et 5 ans pour les créances passées en perte.

La Commission a indiqué dans sa délibération rendue en 1989 sur le projet de loi relatif à la prévention et au règlement judiciaire des difficultés liées au surendettement des ménages[21] que la recommandation de 1988 constituait le socle de garanties minimales à respecter lors de la mise en oeuvre d'un fichier central dans le secteur du crédit.

◦ cette époque, la Commission avait également souhaité que la création d'un fichier central géré par les pouvoirs publics soit de nature à limiter la prolifération des autres fichiers de ce type et que l'on aboutisse à un fichier unique détenu par la Banque de France. Ce dernier point n'a pas été consacré par la loi du 31 décembre 1989 [22] qui n'interdit pas aux organismes professionnels ou aux organes centraux représentant les établissements de crédit de tenir d'autres fichiers communs que celui dont la loi a confié la gestion à la Banque de France

Un fichier commun de lutte contre la fraude est beaucoup plus sensible qu'un fichier commun d'impayés. L'impayé est un fait objectif et de nature civile. La fraude est évidemment beaucoup plus subjective et de nature pénale.

En outre, le secteur du crédit est soumis au secret bancaire qui impose des obligations particulières. Certes, dans certains pays étrangers, de tels fichiers existent, trouvant leur fondement dans un prétendu consentement des personnes. Mais peut-on soutenir que le consentement ou l'autorisation de lever le secret bancaire pour autoriser la communication d'informations relatives au crédit dans un fichier central est librement consenti, lorsque l'on n'a d'autre choix que d'y consentir pour que sa demande de crédit soit examinée ?

Enfin, il est inutile de préciser à quel point l'inscription dans un tel fichier est stigmatisante et peut créer un préjudice pour les personnes fichées à tort ou finalement rétablies dans leur droit par une décision de justice. ◦ supposer même que la fraude soit patente, pendant combien de temps est-il légitime qu'un comportement fautif soit conservé dans un fichier national ?

L'ensemble de ces observations milite, en tout état de cause, en faveur d'un encadrement législatif précis concernant les conditions d'inscription, la durée de conservation et les droits des personnes, un tel fichier, s'il s'avérait indispensable à la profession et socialement admis, devant en outre être placé sous le contrôlé d'une autorité publique telle que la Banque de France.

La directive du 24 octobre 1995 relative à la protection des données personnelles y invite en précisant dans son article 8-5 qu'un fichier « d'infractions » peut

[20] Qui peut être déterminé par référence aux normes de la Commission bancaire.
[21] Délibération n° 89-108 du 26 septembre 1989, 10e rapport annuel, p. 127.
[22] Loi n°89-1010 relative à la prévention et au traitement judiciaire des difficultés liées au surendettement des particuliers et des familles, JO 2 janvier 1990, p. 18.

être mis en œuvre dans le secteur privé, uniquement à la condition que des garanties appropriées soient réunies et sous le contrôle de l'autorité publique.

I. Où l'on reparle du fichier positif

A l'occasion de ces missions de contrôle, a été reposée la question de l'appréciation par les institutions financières de la capacité de remboursement des emprunteurs au moyen d'un fichier recensant les encours de toutes les personnes auxquelles un crédit a été consenti (fichier dit « positif ») et non d'un fichier recensant les seules personnes n'ayant pas honoré leurs échéances (fichier dit « négatif »).

Il serait vain d'ignorer que l'environnement européen et international est clairement orienté vers les fichiers « positifs ». Les arguments au soutien de la création de tels fichiers ne manquent pas de force. Un fichier « positif » est tout d'abord beaucoup moins stigmatisant qu'un fichier « négatif » puisque, par définition, tous les emprunteurs y figurent. La meilleure connaissance de la situation d'un emprunteur qui résulterait de l'analyse financière de son comportement à partir d'éléments exhaustifs et objectifs pourrait éviter certaines méthodes d'appréciation du risque beaucoup plus intrusives ou ne reposant que sur la statistique et le « profil » supposé d'une personne (scoring) et conduire en définitive à accorder des crédits à de nouvelles catégories de population, pour l'heure le plus souvent exclues du crédit, telles que les ménages à faibles revenus, les jeunes, les étrangers, etc.

◦ ces arguments qui ne sont, pour l'heure en France, soutenus que par une importante société financière favorable à l'introduction sur le marché français des pratiques inspirées des *crédit bureau* américains, peuvent être opposés des arguments en sens contraire.

Ainsi, la CNIL, en 1989 et après avoir entendu le gouverneur de la Banque de France et le secrétaire d'Etat à la consommation, a considéré qu'un fichier ne recensant que les incidents de paiement présentait moins de risque pour la vie privée. Le Comité consultatif des usagers créé par la loi bancaire était d'ailleurs du même avis. Un fichier « positif » enregistrant des informations sur tous les crédits souscrits par une même personne comporte des éléments patrimoniaux et de mode de vie qui relèvent en tant que tels de la vie privée. Aussi doit-on s'interroger sur la légitimité pour un organisme prêteur d'accéder à de telles données personnelles alors même que l'emprunteur remplit normalement ses obligations contractuelles et n'a pas d'incident de paiement.

La question de l'efficacité d'un fichier « positif » a d'ailleurs toujours été posée. Des personnes fortement endettées peuvent grâce à une gestion rigoureuse de leur budget faire face à toutes les échéances de leurs emprunts alors que des ménages peu endettés peuvent être à l'origine d'incidents de paiement. Ainsi, le taux d'impayés au Royaume-Uni qui dispose pourtant de deux centrales « positives » est de même niveau qu'en France.

Un fichier « positif » se prête plus facilement à des détournements de finalité qu'un fichier « négatif » tant le nombre et la richesse des informations qu'il comporte peut nourrir la tentation de l'utiliser à d'autres fins.

Un fichier « positif » peut avoir 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, le relatif isolement de la France à cet égard n'est peut être pas aussi significatif qu'il y paraît. De nombreux pays, y compris européens, ne se sont dotés de lois « informatique et libertés » que postérieurement à la constitution de fichiers « positifs », sur l'existence desquels il était difficile de revenir. Dans de nombreux États étrangers, ce sont les dérives des établissements de crédit au regard de la vie privée des personnes qui se trouvent à l'origine d'une réflexion nouvelle sur la nécessité d'adopter une législation protégeant les données personnelles et, force est de constater que les réflexions françaises en la matière rencontrent toujours un assez large écho que l'on ne saurait réduire à leur caractère « exotique ».

Il va de soi que le débat n'est pas clos, même si des considérations qui peuvent être étrangères au souci de la protection des données personnelles expliquent que, dans leur majorité, les établissements de crédit français ne souhaitent pas une telle mise en commun des informations dont ils disposent, considérées comme la richesse propre de l'établissement. Il est vrai que la création d'un fichier positif faciliterait l'entrée sur le marché français de sociétés étrangères ou la création de nouveaux établissements qui pourraient disposer, d'emblée, d'une information précieuse, déjà collectée et centralisée.

La Commission a décidé, sur la base de cette étude relative à la prévention de la fraude et des impayés dans le secteur du crédit à la consommation, de procéder à une large consultation tant auprès des professionnels, des associations de consommateurs que des autorités régulatrices du secteur.

Chapitre 8

LA MONDIALISATION

DE LA PROTECTION

DES DONNÉES

La 22e conférence internationale des commissaires à la protection des données qui s'est tenue à Venise en septembre 2000 avait pour titre emblématique « Un monde, une protection des données ».

Le propos de ce chapitre n'est pas de faire la synthèse de toute l'activité mondiale de l'année en matière de protection des données, ce qui dépasserait le cadre d'un rapport d'activité[23] , mais d'indiquer les faits les plus marquants qui laissent penser, en effet, que l'année 2000 pourrait être considérée comme une année charnière vers une véritable mondialisation de la protection des données, l'Europe continuant à jouer dans ce domaine le rôle de pointe qu'elle tient depuis les années 70.

Outre le fait que les instances nationales coopèrent de plus en plus au plan mondial pour mieux « penser mondial et agir local ou régional », après les cinq années qui nous séparent tout à la fois, de la première réunion du *G7* sur la société de l'information organisée à sa demande à Bruxelles en février 1995 par la Commission européenne et qui avait conclu notamment à l'engagement des parties à assurer de manière effective la protection de la vie privée et des données personnelles au plan national et régional, de l'adoption par l'Union européenne quelques mois après de la directive 95/46/CE du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, et de la « privatisation » d'Internet, deux des partenaires économiques de premier plan de l'Europe, le Canada et l'Australie, ont rejoint en l'an 2000 le club des États protecteurs sur le

[23] Pour avoir une vue d'ensemble détaillée de la protection des données dans le monde, outre la consultation de l'annexe au présent rapport donnant les références aux législations de protection des données adoptées dans le monde à ce jour, on pourra consulter également avec profit, par exemple à partir des liens établis sur le site web de la CNIL (www.cnil.fr), tous les sites Internet des autorités de protection des données que ces législations ont instituées, et pas seulement en Europe, ainsi que le site de la Commission européenne sur lequel sont diffusés tous les textes adoptés par le groupe consultatif des autorités indépendantes institué au plan européen par l'article 29 de la directive 95/46CE du 25 octobre 1995.

fondement d'une législation applicable y compris dans le secteur privé. L'annonce de l'adoption de ces textes a fait chaque fois référence notamment à la directive précitée de l'Union européenne. Par ailleurs, des progrès sont également maintenant réalisés dans d'autres États y compris du sud, en Argentine en particulier. Au total, 50 États ont adopté à ce jour des législations en matière de protection des données personnelles (point I).

Le rôle de pointe tenu par l'Europe est également révélé par l'analyse de nombreuses mesures intervenues cette année au sein de l'Union européenne en vue d'établir un système cohérent de protection des données à caractère personnel, tout en tenant compte des particularités de la construction européenne : transposition des directives par les États-membres, adoption par le Parlement européen et le Conseil du règlement pour les institutions et organes communautaires, proclamation par le Parlement européen, le Conseil et la Commission de la Charte des droits fondamentaux, sous présidence française, décisions de la Commission européenne en matière de transferts de données vers des pays tiers, travaux du groupe consultatif des autorités de protection des données institué par l'article 29 de la directive 95/46/CE, travaux, enfin, des autorités communes de protection des données dans les activités de l'Union relevant du troisième pilier (point II).

On observera toutefois que les médias n'accordent peut-être pas suffisamment d'attention au rôle de premier plan joué par l'Europe dans ce domaine, préférant accorder plus d'attention aux aspects potentiellement conflictuels inter-étatiques ou intercontinentaux (États-Unis/Europe par exemple) ainsi qu'aux « scandales » (annonces des projets de ventes de fichiers commerciaux de jeunes entreprises Internet américaines en faillite par exemple). Ces faits constituent certes autant d'aiguillons dans le domaine de la protection des données, mais ils ne permettent pas à eux seuls de rendre compte de l'importance du lent mais décisif travail réalisé en profondeur en Europe, dans lequel sont impliqués l'ensemble de ses instances décisionnelles.

Dans ce contexte, la CNIL a souhaité contribuer à une meilleure visibilité de l'ensemble des travaux réalisés dans le monde. C'est pourquoi dans le cadre de la préparation de la 23^{e} conférence internationale des commissaires à la protection des données qu'elle organise à Paris du 23 au 26 septembre 2001, elle a lancé un « journal » de la conférence internationale largement diffusé sur support papier et électronique et que l'on peut consulter sur son site web.

I. L'ESSOR DES LOIS DE PROTECTION DES DONNÉES PERSONNELLES HORS D'EUROPE

L'année 2000 a été marquée par une nouvelle étape dans le développement de la protection des données sur tous les continents.

Deux des grands partenaires commerciaux de l'Europe, le Canada et l'Australie qui, s'ils assuraient par la législation jusqu'ici la protection des personnes à l'égard des données à caractère personnel dans le secteur public ont opté, après plusieurs années d'hésitation[24] , pour l'adoption d'une législation fédérale couvrant le secteur privé.

La loi canadienne « sur la protection des renseignements personnels et les documents électroniques » a été adoptée le 13 avril 2000 et est entrée en vigueur le 1er janvier 2001 (http ://www.privcom.gc.ca). Elle est d'application dans les secteurs privés réglementés au niveau fédéral (transport aérien, banques, radiodiffusion, transport inter-provinciaux, télécommunications) et concerne toutes les données ou renseignements personnels. Elle devrait s'appliquer également à tout autre secteur privé d'ici trois années dans les provinces qui n'auraient pas d'ici là adopté de législation assurant une protection équivalente. Le commissaire fédéral à la protection des données est compétent pour les secteurs privés relevant du niveau fédéral.

En Australie, la législation fédérale de 1988, qui concerne le secteur public, a été amendée le 6 décembre 2000 de sorte que les données personnelles feront à partir du 21 décembre 2001 l'objet d'une protection dans la quasi-totalité des activités commerciales du secteur privé, mais ne concerne pas les données relatives aux employés (www.privacy.org.gov). Les professionnels sont encouragés à élaborer des codes de conduite fondés sur les principes posés par la loi, incluant, s'ils le souhaitent, des instances de règlement des litiges, et à les soumettre pour approbation au commissaire fédéral à la protection des données, ce dernier étant par défaut l'instance de règlement des litiges.

En Argentine, la loi de protection des données a été promulguée le 2 novembre 2000 et est d'application tant dans le secteur public que dans le secteur privé. La commission qu'elle institue devrait être installée en 2001.

La consultation lancée par le gouvernement sud-africain sur le commerce électronique, sous forme de livre vert, inclut un chapitre sur la protection des consommateurs et la vie privée. Il se réfère à l'exemple de plus de 50 pays qui ont déjà adopté une législation dans ce domaine. Cette approche, qui pourrait se concrétiser en un projet de loi lors de la publication du livre blanc qui fera suite à la consultation, viendrait ainsi compléter le droit d'accès des personnes concernées aux données les concernant (secteur public et secteur privé), garanti par une loi du 2 février 2000, pour laquelle la Commission des droits de l'homme prévue par la constitution est compétente.

En ce qui concerne le Japon, le gouvernement poursuit ses travaux préparatoires à une législation fixant des principes de base.

Enfin, aux États-Unis, la phase « autorégulation » paraît atteindre ses limites.

Alors que la justice est saisie et sanctionne de plus en plus de cas d'atteinte aux droits des consommateurs en matière de protection des données sur le fondement d'une pratique décevante (non-respect de la politique de protection des données

[24] 20e rapport d'activité de la CNIL 1999, p. 185.

énoncée par l'entreprise), de plus en plus de propositions législatives sont déposées tant au niveau étatique (plus de 300 propositions) que fédéral (plus de 20 propositions).

Au printemps 2000, après l'entrée en vigueur de la loi fédérale sur la protection de la vie privée des enfants sur Internet (dite « COPRA »), la Federal Trade Commission, compétente pour la mise en œuvre de cette législation, a publié une étude montrant à la fois les progrès réalisés mais également les difficultés de l'autorégulation dans les autres domaines de la protection de la vie privée en ligne et a conclu, à l'occasion de sa déposition devant le Congrès, à la nécessité de passer à une phase législative.

Dans l'industrie électronique, en particulier, les responsables des sociétés (tout d'abord Hewlett Packard, puis Intel et IBM) se sont déclarés également, au cours du second semestre 2000, en faveur d'une législation fédérale mais prévalant sur les éventuelles législations des Etats pour éviter la fragmentation du marché.

Les deux candidats à la Maison Blanche, Georges W. Bush et Al Gore, ont fait au cours de la campagne électorale de l'année 2000 des déclarations d'attachement à la protection de la vie privée et des données à caractère personnel mais peu précises en terme de plan d'action.

Pour sa part, Bill Clinton a promulgué quelques semaines avant son départ une réglementation concernant la protection des données médicales, qu'il estime insuffisante, le travail restant, notamment dans le secteur des assurances, relevant du Congrès qu'il incite à agir.

De plus, de l'examen des propositions de lois en instance il ressort que cette préoccupation est partagée tant par les démocrates que par les républicains.

Le Congrès devrait être sans doute le lieu où, dès 2001, des discussions importantes sur le sujet devraient prendre place. La question de la nécessité ou non de légiférer parait désormais dépassée. Les débats, voire les conflits qui ne manqueront pas d'apparaître sous la pression de certains acteurs du secteur privé, divisés sur le sujet, porteront non sur l'opportunité de légiférer mais sur le contenu d'une ou plusieurs possibles législations (selon la tradition américaine des lois sectorielles) après examen des questions soulevées de manière parcellaire par toutes les propositions de lois en instance. Seront ainsi en débat tous les éléments d'un système de protection, le champ d'application de la protection nouvelle à instaurer (activités commerciales en ligne et/ou hors ligne, autres activités, réexamen des protections assurées dans le secteur financier et dans le secteur public, notamment non fédéral), la portée d'une possible loi fédérale en matière commerciale (prévaudra-t-elle ou non sur les législations des États ?), les obligations des détenteurs de données personnelles, les droits des personnes (portée du consentement/droit d'opposition en matière de marketing direct, droit d'accès, etc.), la place des codes de déontologie et les pouvoirs de l'autorité ou des autorités indépendantes qui seraient compétentes, les recours des personnes et les sanctions.

II. LES TRAVAUX AU SEIN DE L'UNION EUROPÉENNE

L'Union européenne se dote peu à peu d'un système complet de protection des données personnelles. Celui-ci est relativement complexe compte tenu des particularités de la construction communautaire qui distingue, d'une part, les activités qui relèvent du droit communautaire, d'autre part, les activités qui relèvent du titre VI du traité (coopération policière notamment) et enfin celles des institutions et organes des communautés européennes (Commission européenne, Parlement européen, Conseil, Comité économique et social, Comité des régions, Cour de justice des communautés, toutes les agences sectorielles, etc.). Cette complexité est reflétée dès lors non seulement par l'existence de différents textes régissant la matière, mais également de différentes institutions pour leur mise en œuvre cependant que la référence commune en matière de protection des données tend à être constituée essentiellement par les directives adoptées par le Parlement européen et le Conseil en 1995 et 1997 (directive « générale » 95/46/Œ du 24 octobre 1995, directive complémentaire « télécom » 97/66/CE du 15 décembre 1997).

Enfin, afin d'éviter le contournemenf de la protection assurée en interne, l'Union européenne se préoccupe du sort réservé aux données à caractère personnel lorsqu'elles sont susceptibles d'être transférées hors de l'Union.

A. Le développement d'un système de protection

1) État de la transposition *des* directives sur (a protection des données à caractère personnel.

La transposition en droit interne de la directive *95/46/CE* du 24 octobre 7 995 a été réalisée à ce jour dans onze États membres. Les quatre autres États membres, l'Allemagne, la France, l'Irlande, le Luxembourg ont fait l'objet d'une procédure devant la Cour de justice de Luxembourg pour manquement à la notification, avant la date prévue par la directive, des mesures prises pour sa transposition. Le contrôle par la Commission de la conformité de ces transpositions n'a pas commencé.

En ce qui concerne la directive 97/66/CE du 15 décembre 1997 relative à la protection de la vie privée et des données à caractère personnel dans le secteur des télécommunications, la non-transposition a également fait l'objet d'une procédure pour manquement à l'issue de laquelle la France a été déclarée en situation de manquement.

2) L'adoption du règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques
à l'égard du traitement des données à caractère personnel
par les institutions et organes communautaires et à la libre circulation de ces données.

Le règlement a été adopté le 18 décembre 2000 et publié au JOCE L 8 du 12 janvier 2001, page 1.

Ce règlement, dont le principe a été prévu dans le cadre du traité d'Amsterdam (article 286 du traité instituant la Communauté européenne), adapte les dispositions des deux directives précitées aux institutions et organes communautaires. Il prévoit un système de mise en œuvre comportant les caractères essentiels ci-après.

1 — Seront créés des délégués à la protection des données désignés en interne par chaque institution et organe communautaire (article 24) ;

2 — Une autorité de contrôle indépendante, dénommée « contrôleur euro péen » et dotée d'un contrôleur adjoint, chargée de l'application du règlement est instituée. Il est confié à cette autorité de larges missions et elle dispose à cet égard de pouvoirs d'intervention également très larges (chapitre V, article 41 à 48). Elle conseille les personnes, instruit les plaintes, contrôle préalablement certaines catégo ries de traitements envisagés (article 27), effectue des contrôles *a posteriori,* coopère avec les autorités nationales de protection des données et avec les autorités de con trôle commune du troisième pilier en tant que de besoin, participe aux travaux du groupe des autorités de protection de données prévu par l'article 29 de la directive 95/46, peut ordonner la rectification et la destruction de données, interdire tempo rairement ou définitivement un traitement, saisir pour sanction la Cour de justice des Communautés européennes et intervenir dans les affaires portées devant la Cour, établit un rapport annuel présenté au Parlement européen, au Conseil et à la Commis sion et qui est publié. Le contrôleur et le contrôleur adjoint sont nommés d'un commun accord, par le Parlement européen et le Conseil, pour une durée de cinq années (renouvelable) sur la base d'une liste établie par la Commission à la suite d'un appel public à candidature. Le premier appel à candidature devrait avoir lieu au premier semestre 2001. Ils seront choisis parmi des personnes ayant une expérience notoire en la matière, tels que des membres ou anciens membres des autorités nationales de contrôle de la protection des données. Cette autorité disposera d'un budget propre et d'un secrétariat dont le personnel sera nommé par le contrôleur européen et soumis aux règlements et réglementations applicables aux fonctionnaires et autres agents des Communautés européennes.

3 — Des sanctions peuvent être infligées par la Cour de justice des Commu nautés européennes.

3) L'installation de l'autorité de contrôle commune prévue par la convention « douane » et la poursuite des travaux en vue d'une approche « horizontale » pour les aspects de protection des données dans les domaines relevant du titre VI du traité de l'Union, c'est-à-dire en matière notamment de coopération intergouvernementale policière et douanière.

— Les travaux se sont poursuivis pour la mise en place de l'autorité de con trôle commune pour le SID (système d'information douanier) qui sera mis en œuvre par la Commission mais qui relève pour partie des compétences communautaires et pour partie de l'intergouvememental (titre VI du traité[25]. Les autorités nationales en charge de la protection des données ont désignés en 2000 leurs représentants et déjà préparé un projet de règlement intérieur de l'autorité de contrôle commune qui devrait être adopté lors de son installation officielle en 2001.

— A été adopté en décembre 2000 le règlement du Conseil « EURODAC » destiné à la centralisation et à la consultation par les autorités nationales compé tentes des empreintes digitales de certaines catégories d'étrangers, les demandeurs du statut de réfugié et les étrangers en situation irrégulière. Ce règlement étant com munautaire, il prévoit le contrôle de la protection des données par le contrôleur euro péen (cf. supra).

— En ce qui concerne l'approche « horizontale », c'est-à-dire le rapproche ment institutionnel et sur le fond, des dispositions de protection des données dans ces divers instruments, le principal progrès réalisé en 2000 est celui découlant de la déci sion du Conseil du 17 octobre 2000 portant création d'un secrétariat commun pour les autorités de contrôle communes pour Europol, Schengen et SID. Ces autorités siè gent maintenant dans les locaux du Conseil à Bruxelles et tiennent leurs réunions « dos à dos » pour tenir compte du fait que les représentants des autorités de contrôle nationales désignés pour participer à ces travaux sont le plus souvent les mêmes.

4) La proclamation de la charte des droits fondamentaux de l'Union européenne

En vue de parachever l'édifice, dans le cadre de la préparation de la Charte des droits fondamentaux, dont le principe et le calendrier avaient été fixés par le Conseil européen de Cologne en juin 1999, le groupe consultatif des autorités européennes de protection des données a dès le 7 septembre 1999 recommandé que le droit à la protection des données à caractère personnel soit inscrit comme droit fondamental particulier. Il dépasse, en effet, la question de la vie privée et doit être régi par des principes particuliers tant il s'agit, en réalité, de protéger, au titre des leurs données à caractère personnel notamment dans le cadre de la société de l'information, l'identité des personnes concernées.

La charte contient désormais ce droit fondamental.

[25] 20e rapport annuel 1999, p. 189.

La charte a été proclamée solennellement, en marge du sommet du Conseil européen de Nice le 7 décembre 2000, par le Parlement européen, le Conseil et la Commission et publiée au JOCE C 354 du 18 janvier 2001, page 1. Elle comporte, après l'article 7 relatif à la protection de la vie privée et familiale, un article spécifique relatif au droit à la protection des données à caractère personnel. Ce droit marque le choix de l'Europe d'ancrer la protection des données dans la protection des droits fondamentaux face au développement de la société de l'information. Ainsi, la Charte énonce, sans qu'il soit besoin de commenter les dispositions tant on y reconnaîtra les principes de base bien connus de la protection des données à caractère personnel, à l'article 8 que :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

B. La coopération entre les autorités européennes de protection des données

La coopération entre les autorités européennes de protection des données est organisée, à la fois dans un cadre « interindividuel » prévu par la directive 95/46/CE (article 28, paragraphe 4) notamment en matière de traitement de plaintes relatif à des traitements de données transfrontaliers, et dans un cadre collectif, manifesté par le groupe consultatif institué par l'article 29 de ladite directive, pour les activités qui relèvent du droit communautaire, et par les autorités de contrôle communes instituées par les diverses conventions passées entre les Etats membres relevant du titre VI du traité, c'est-à-dire essentiellement en matière de contrôle policier.

1) Les travaux du groupe consultatif dit de l'article 29

Au cours de l'année le groupe, dont le président élu pour deux années en l'an 2000 est le président de la Commission italienne, M. Stefano Rodota, s'est réuni à Bruxelles au moins une fois tous les deux mois et a adopté neuf recommandations et avis en relation essentiellement avec ces deux missions principales (article 28 de la directive) :

contribuer à l'application homogène des directives, notamment par des initiatives propres, ce que le groupe a fait essentiellement dans les domaines les plus internatio naux et en pleine mutation que sont les télécommunications, Internet, le génome hu main ;

donner son avis sur le niveau de protection des pays tiers notamment dans le cadre de travaux préparatoires aux décisions de la Commission de reconnaissance du niveau adéquat de protection assuré dans les pays tiers prévues à l'article 25 de la directive 95/46/CE.

On observera que malgré le dialogue entretenu avec les organisations professionnelles, le groupe n'a pas été encore en mesure de donner d'avis favorables sur les codes de conduite professionnels qui lui ont été présentés.[26]

On notera le pragmatisme des méthodes de travail utilisées pour préparer les délibérations du groupe qui repose, soit sur l'initiative du secrétariat animé par la Direction marché intérieur Commission européenne, soit sur la présentation de textes préparés par telle ou telle délégation nationale particulièrement intéressée par un sujet, soit, notamment en ce qui concerne les activités télécommunications et Internet, sur les travaux de sous-groupes de travail auxquels participent les représentants des autorités de contrôle nationales qui le souhaitent.

Internet

Le groupe a poursuivi ses activités des années précédentes en complétant les travaux antérieurs sur des questions majeures soulevées par Internet, les données publiques et sur la conservation des données de connexion, de deux manières. D'une part, il a inscrit à l'ordre du jour, sur proposition française, un troisième sujet d'enjeu particulier, celui de la prospection commerciale par e-mail en relation tant avec l'actualité nationale qu'européenne des travaux d'élaboration de la directive sur certaines aspects du commerce électronique. Il a d'autre part élaboré un volumineux document de synthèse à vocation pédagogique.

Les sollicitations commerciales par e-mail

Sur proposition de la CNIL, faisant suite à la publication de son rapport sur le publipostage électronique le 14 octobre 1999[27] , et afin de clarifier les questions de protection des données soulevées par la proposition de directive sur certains aspects du commerce électronique, le groupe a adopté le 3 février 2000, préalablement à l'adoption de sa position commune par le Conseil, un avis qui consacre l'analyse faite par la CNIL dans ce domaine. L'avis précise qu'est contraire au principe de la protection des données la collecte d'e-mail dans les espaces publics d'Internet et que la collecte loyale des e-mail à des fins de prospection repose sur l'information claire et préalable à la communication de celles-ci par les personnes concernées et à l'offre par un moyen simple, une case à cocher par exemple, d'exprimer leur choix.

Le document de travail de synthèse sur le respect de la vie privée sur Internet : une approche européenne intégrée de la protection des données en ligne

Sur la base d'un important travail préparatoire effectué par la « task force Internet » du groupe de travail au cours de l'année, à laquelle la CNIL participe activement, le groupe a pu adopter et publier le 20 novembre 2000 un « Document de travail sur le respect de la vie privée sur Internet : une approche européenne intégrée

[26] L'ensemble des recommandations, avis et documents de travail adoptés par le groupe sont accessibles sur le site europa de la Commission européenne à l'adresse http ://europa.eu.int/comm/internal-market/fr/media/dafaprot/wpdocs.

[27] Cf. 20e Rapport annuel d'activité 1999, p. 107

de la protection des données en ligne. » Ce document de travail de synthèse est à vocation essentiellement pédagogique. Il s'attache à décrire les processus techniques au regard du rôle des différents acteurs, à identifier les risques particuliers pour la vie privée, à analyser les solutions du point de vue juridique et technique en application de la réglementation européenne au regard des différents types d'usages rencontrés sur Internet, courrier électronique, recherche d'informations, publication et forum, transactions.

Les recommandations finales concernent la nécessité :
d'améliorer la connaissance des utilisateurs des questions traitées, de leurs obli gations et droits ;
de contribuer à une conception et une diffusion de produits techniques plus res pectueux des principes de la protection des données ;
de mettre au point des mécanismes de contrôle efficace du respect des disposi tions européennes notamment en élaborant une liste de points de contrôle destinés à faciliter l'auto évaluation par les sites et leur labellisation sur la base de critères euro péens. ◦ cette fin, la CNIL a fait parvenir au mois de décembre 2000 un document de travail, discuté en début d'année 2001.

La révision de la directive 97/66 du 15 décembre 1997 sur la protection de la vie privée et la protection des données dans le secteur des télécommunications

La Commission a proposé, dans le cadre d'une consultation publique en début d'année suivie de l'adoption de plusieurs propositions de directives en juillet 2000, de réviser le cadre réglementaire des télécommunications en vue de le simplifier (passage de 20 directives à 5 directives), d'améliorer les conditions de la concurrence dans ce secteur, et de le moderniser pour tenir compte de la convergence des technologies de communication.

Dans ce contexte, elle a adopté le 12 juillet 2000 une proposition de directive du Parlement européen et du Conseil (Corn (2000) 385) destinée à modifier certaines des dispositions de la directive 97/66/CE du 15 décembre sur la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications pour l'étendre notamment à l'ensemble du secteur des communications électroniques, c'est-à-dire incluant les fournisseurs de services Internet et les services de télévision interactifs.

Le groupe a procédé à un premier examen des modifications proposées dont les résultats ont été rendus publics sous la forme d'un avis le 2 novembre 2000.

Le groupe de l'article 29 a exprimé son soutien en ce qui concerne l'élargissement du régime de protection à toute l'infrastructure de communication en raison de la nécessité de conférer le même degré de confidentialité aux communications effectuées quelle que soit la nature du réseau utilisé.

Il a cependant réitéré son souhait exprimé l'année précédente (avis du 3 septembre 1999 sur la conservation des données dites de « trafic ») que soit fixé de manière harmonisée le délai pendant lequel une facture de communication peut être

contestée. Ce délai est extrêmement variable au sein des États-membres (allant de 15 jours à dix ans) et parfois au sein d'un même État-membre en fonction du statut de l'opérateur concerné. Or, ce délai fixe, en application du principe de proportionnalité, la période pendant laquelle peuvent être légitimement conservées, au-delà de l'établissement de la communication, certaines données sur le détail des communications telles que les numéros appelés nécessaires aux fins de preuve de la facturation en fonction de la consommation.

De même, le groupe soutient l'inversion proposée par la Commission du principe à la base jusqu'à présent de la constitution des annuaires, consistant à abandonner l'obligation faites aux abonnés et aux usagers des réseaux publics à figurer dans un annuaire et à lui substituer le principe de l'inscription volontaire.

Cependant, le groupe a fait part de son souhait de voir établir des mesures de protection pour tenir compte de l'évolution des services d'annuaires et des risques qu'ils font peser sur la vie privée :

— maintien de la protection à l'égard des usages non souhaités des données conte nues dans les annuaires ou cédées par les opérateurs à des fins de prospection,

— consentement des personnes concernées à l'élaboration de services d'annuaires inversés au moyen desquels les noms et adresses des personnes peuvent être décou verts à partir d'un simple numéro de téléphone [28]

— fixation de la période de validité de la licence d'usage accordée aux utilisateurs d'annuaires diffusés sur CD ROM afin de tenir compte des modifications apportées par les personnes concernées dans les choix qu'elles expriment à l'égard de ces dif férents usages (retrait éventuel d'un annuaire et des annuaires inversés, des cessions de listes à des fins de prospection).

En matière de facturation détaillée, le groupe souhaite le maintien des dispositions relatives à la possibilité qu'a un abonné de recevoir celles-ci avec la liste de ses appels sans toutefois qu'apparaissent les quatre derniers chiffres du numéro appelé.

En matière de localisation des mobiles, le groupe soutient la proposition de la Commission européenne. Celle-ci estime que la donnée de localisation, lorsqu'elle est générée aux fins de l'établissement d'un appel et qu'elle a le même statut que les autres données de trafic. Par contre, lorsque la localisation d'un mobile est calculée par un opérateur pour fournir des services dits à valeur ajoutée, le groupe a considéré qu'il convenait de tenir compte de sa très grande sensibilité puisqu'elle touche à la liberté d'aller et venir alors même qu'elle n'est pas nécessaire à l'établissement d'une communication. C'est pourquoi il a estimé, dans une première approche sur laquelle il se réserve de revenir pour tenir compte des expériences très récentes dans le domaine, que cette donnée ne devait être collectée et transmise dans le réseau et éventuellement vers un fournisseur externe de services, voire à un particulier, qu'avec le consentement de l'intéressé exprimé à partir de son terminal, d'autant que la

[28] L'émergence de ces services, à l'insu des personnes concernées, a donné lieu dans plusieurs ɜtats-membres à de nombreuses plaintes. La liberté de circulation de ces services, établis de plus en plus sur une base européenne et non plus simplement nationale, rend dès lors l'harmonisation nécessaire.

technologie en cause peut en théorie être mise en oeuvre à l'insu de la personne concernée.

En matière de prospection par e-mail, le groupe soutient la proposition de la Commission de subordonner de telles opérations au consentement préalable de la personne concernée, comme la réglementation le prévoit déjà en matière d'usage d'automates d'appels et de télécopieur.

2) La coopération au sein des autorités de contrôle communes

Cette coopération a donné lieu, principalement en ce qui concerne les systèmes « Schengen » et Europol [29] , à des contrôles sur place effectués par les autorités de contrôle communes en octobre 2000. Les rapports élaborés ont été transmis pour observation respectivement au ministère de l'Intérieur français en charge du fichier commun tenu à Strasbourg et au Conseil d'administration et au directeur d'Europol.

C. Les transferts de données personnelles vers les pays tiers

Le cadre juridique de l'Union européenne en la matière est défini par les articles 25 et 26 de la directive 95/46/CE rappelés par la CNIL dans son 20e rapport annuel (p. 200).

Il repose sur le principe du transfert de données vers des pays assurant une protection « adéquate ». Ce principe est assorti de dérogations, notamment lorsque le destinataire des données présente des garanties suffisantes, résultant notamment de la conclusion d'un contrat comportant des clauses appropriées types. Le contrôle de la conformité est du ressort des Etats-membres.

En vue de développer une politique cohérente, la directive confère à la Commission européenne un pouvoir réglementaire dans deux cas : celui de reconnaître l'adéquation du niveau de protection assuré dans un pays tiers, et celui d'adopter des clauses contractuelles types. Ce pouvoir est exercé sous le contrôle d'un comité de représentants des États-membres, le comité dit « 31 » (du numéro de l'article de la directive qui l'institue) et après avis du groupe des autorités indépendantes de contrôle nationales.

Le 27 juillet 2000 la Commission a pris, selon cette procédure, ses trois premières décisions de reconnaissance du niveau adéquat de protection publiées au JOCE L/235 du 24 août 2000.

Elles ont concerné tout d'abord la Suisse et la Hongrie, qui ont adopté des législations en matière de protection des données et sur lesquelles le groupe de l'article 29 avait rendu des avis favorables respectivement les 7 juin et 7 septembre 1999.

[29] Pour le détail, voir le 20e rapport annuel de la CNIL 1999, p. 187.

Elles ont concerné également le dispositif particulier dit de la « sphère de sécurité » américain qui a été longuement décrit dans le rapport annuel d'activité de la CNIL 1999 (page 200). Le département du commerce a ouvert le 2 novembre 2000 aux entreprises la procédure d'inscription sur la liste publique de celles qui ont adhéré au dispositif , qui précise le domaine d'activité couvert et l'organisme de résolution des litiges compétent. Le département américain du commerce n'a cependant commencé à largement diffuser l'information sur le dispositif[30] qu'en fin d'année, si bien que seules une dizaine d'entreprises étaient inscrites fin décembre 2000. Cette liste est consultable par Internet à l'adresse :
http ://web.ita.doc.gov/safeharborshlist.nsf/webPages/safe+harbor+list.

Par ailleurs, le groupe de l'article 29 a pu examiner en décembre 2000 la nouvelle situation canadienne et a rendu son avis lors de sa première réunion de 2001. Il observe que toute décision sur le niveau de protection assuré par la loi canadienne doit tenir compte des limites de son champ d'application et du calendrier de sa mise en œuvre. Il invite aussi la Commission à approfondir les interactions entre la loi fédérale et les lois provinciales. Il invite les autorités canadiennes à poursuivre les efforts pour améliorer le niveau de protection des données. Le groupe a également examiné la situation australienne qui présente, malgré l'adoption de la loi, quelques difficultés justifiant un complément d'analyse ; ces difficultés pourraient cependant se résoudre notamment grâce au dispositif prévu pour l'élaboration et l'adoption de codes de conduite professionnels.

Enfin, la Commission en étroite collaboration avec le groupe de l'article 29 a engagé ses travaux en vue de l'adoption de clauses contractuelles types. Ces travaux, largement avancés, devraient déboucher avant la fin du premier semestre 2001.

[30] Pour la consultation des principes et des procédures établies aux USA tels que publiés par le département du commerce, se reporter à www.ita.doc.gov/td/ecom/menu.html.

ANNEXES

Annexe 1

Composition de la Commission au 15 mai 2001

Président : **Michel GENTOT,** président de section au Conseil d'État

Vice-président délégué : **Hubert BOUCHET,** membre du Conseil économique et social

Vice-président : **Gérard GOUZES,** député du Lot-et-Garonne, maire de Marmande

Commissaires :

Cécile ALVERGNAT, directrice générale de l'Echangeur

Maurice BENASSAYAG, conseiller d'État

André BOHL, sénateur de la Moselle, maire de Creutzwald

Didier GASSE, conseiller maître à la Cour des comptes

François GIQUEL, conseiller maître à la Cour des comptes

Pierre LECLERCQ, conseiller à la Cour de cassation

Philippe LEMOINE, président directeur général de Laser, membre du directoire des Galeries Lafayette

Jean-Pierre de LONGEVIALLE, conseiller d'État

Marcel PINET, conseiller d'État honoraire

Guy ROSIER, conseiller maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social, adjoint au maire de Paris.

Alex T-RK, sénateur du Nord

Alain VIDALIES, député des Landes

Maurice VIENNOIS, conseiller-doyen honoraire à la Cour de cassation

Commissaires du gouvernement :

Charlotte-Marie PITRAT

Michel CAPCARRERE, adjoint

Composition de la Commission au

31 décembre 2000

Président : **Michel GENTOT,** président de section au Conseil d'État,

Vice-président délégué : **Hubert BOUCHET,** membre du Conseil économique et social, secrétaire général de l'Union des Cadres et Ingénieurs Force Ouvrière

Vice-président : **Gérard GOUZES,** député du Lot-et-Garonne, maire de Marmande

Commissaires :

Cécile ALVERGNAT, directrice générale de l'Echangeur

Maurice BENASSAYAG, conseiller d'État

André BOHL, sénateur de Moselle, maire de Creutzwald

Noël CHAHID-NOURAJ, conseiller d'État

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Pierre LECLERCQ, conseiller à la Cour de cassation

Philippe LEMOINE, président-directeur général de Laser, co-président du directoire des Galeries Lafayette

Marcel PINET, conseiller d'État honoraire

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social

Alex T-RK, sénateur du Nord

Alain VIDALIES, député et conseiller général des Landes

Maurice VIENNOIS, conseiller-doyen honoraire à la Cour de cassation

Commissaires du gouvernement :

Charlotte-Marie PITRAT, commissaire du gouvernement,

Michel CAPCARRERE, commissaire adjoint du gouvernement,

Annexe 2

Répartition des secteurs d'activité

Hubert BOUCHET, vice-président délégué : emploi, recrutement, formation, élections professionnelles

Gérard GOUZES vice-président : justice (autorité judiciaire, justice administrative, professions judiciaires), autorités administratives indépendantes, archives nationales

Cécile ALVERGNAT : commerce électronique, plate-forme d'intermédiation, modes de paiement sur Internet

Maurice BENASSAYAG : enseignement public et privé, partis politiques, sondages, marketing politique, droit d'accès indirect

André BOHL : recherche en santé et sciences sociales (dont INED)

Didier GASSE : marketing, poste, assurance, renseignement commercial, recouvrement de créance, droit d'accès indirect

François GIQUEL : police nationale, gendarmerie nationale, police municipale, renseignement militaire et civil, service national, affaires étrangères, droit d'accès indirect

Pierre LECLERCQ : fichiers de la Banque de France, fichiers bancaires (notamment segmentation comportementale), banque à domicile, bourse, crédit à la consommation, droit d'accès indirect

Philippe LEMOINE : publicité en ligne, télébillétique, localisation des véhicules, veille technologique

Pierre de LONGEVIALLE : trésor public, fiscalité, cadastre, publicité foncière, douanes, répression des fraudes, comptabilité publique, droit d'accès indirect

Marcel PINET : télécommunications et réseaux dont Internet (notamment fournisseurs d'accès et d'hébergement, diffusion de données publiques sur Internet), sécurité, cryptologie, participation aux groupes de travail internationaux dans ce domaine, participation au groupe européen dit de « l'article 29 », droit d'accès indirect.

Guy ROSIER : enquêtes statistiques mises en œuvre par l'INSEE, culture, jeunesse et sport, tourisme, logement, immobilier, transport, équipement, environnement, industrie, énergies, artisanat, agriculture, droit d'accès indirect

Pierre SCHAPIRA : aide sociale, revenu minimum d'insertion, collectivités locales (gestion des administrés hors fiscal et police municipale)

Alex T-RK : presse, églises, associations, syndicats, coopération européenne et internationale en matière de police, de justice et de douanes

Alain VIDALIES : santé (volet médical de la carte de santé, gestion hospitalière, des cabinets médicaux et paramédicaux, médecine du travail, médecine préventive)

Maurice VIENNOIS : sécurité sociale, assurance vieillesse, assurance maladie, allocations familiales, mutuelles, droit d'accès indirect

Annexe 3

Organigramme des services au 15 mai 2001

Président : **Michel GENTOT**

Secrétaire général, chargé des affaires juridiques : **Joël BOYER,** magistrat

Annexe 4

Liste des délibérations adoptées en 2000

Les délibérations sont publiées dans les chapitres du rapport, à la suite des commentaires qui les évoquent ou en annexe 5. Elles sont signalées dans le tableau suivant, par un renvoi à la page concordante dans le rapport. Le texte intégral de l'ensemble des délibérations de la CNIL, depuis 1978, est accessible par minitel sur le « 3617 jurifrance » ou après abonnement sur le « 3613 JRF », ou par Internet, après abonnement, sur les sites http ://www.jurifrance.com et http ://www.lamyline.com.

Numéro Date	Date et objet
00-001 13 janvier 2000	Délibération portant autorisation de mise en oeuvre par le Comité médical paritaire local des médecins généralistes de Paris d'un traitement de données personnelles de santé ayant pour objet l'évaluation des pratiques médicales de prescription dans la rhino-pharyngite de l'enfant
00-002 13 janvier 2000	Délibération portant autorisation mise en œuvre par l'Agence régionale de l'hospitalisation d'Ile-de-France d'un traitement de données personnelles de santé à des fins d'évaluation des pratiques de soins en urgence face à un infarctus du myocarde
00-003 13 janvier 2000	Délibération portant autorisation de mise en œuvre par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins
00-004 13 janvier 2000	Délibération portant délégation d'attribution au président et au vice-président délégué de la Commission nationale de l'informatique et des libertés
00-005 27 janvier 2000	Délibération portant avis sur un projet d'acte réglementaire présenté par l'UNEDIC portant création d'un fichier national des ASSEDIC
00-006 27 janvier 2000	Délibération portant avis sur un traitement de l'UNEDIC ayant pour finalité la gestion des opérations administratives et techniques relatives à l'inscription des demandeurs d'emploi par les ASSEDIC

Numéro Date	Date et objet
00-007 27 janvier 2000	Délibération portant avis sur le projet de modification du décret 87-1025 du 17 décembre 1987 relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage
00-008 27 janvier 2000	Délibération portant avis sur un projet d'arrêté du premier président de la Cour des comptes relatif à la création d'un traitement automatisé ayant pour finalité le contrôle des rémunérations versées à leur personnel par l'Etat et ses établissements publics
00-009 27 janvier 2000	Délibération portant avis sur une demande d'avis du secrétaire d'État à l'industrie relative à l'article 7 d'un avant-projet de loi portant diverses dispositions d'harmonisation communautaire (article destiné à compléter la transposition en droit français de la directive 97/66 concernant la protection des données à caractère personnel et la vie privée dans le secteur des télécommunications)
00-010 3 février 2000	Délibération 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
00-011 3 février 2000	Délibération décidant un contrôle sur place
00-012 22 février 2000	Délibération décidant un contrôle sur place
00-013 22 février 2000	Délibération portant adoption du formulaire de déclaration des traitements de données personnelles mis en oeuvre dans le cadre d'un site Internet
00-014 9 mars 2000	Délibération décidant un contrôle sur place
00-015 21 mars 2000 (cf. p. 110)	Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à gérer l'accès à la cantine scolaire par la reconnaissance des empreintes digitales

Numéro Date	Date et objet
00-016 21 mars 2000	Délibération décidant un contrôle sur place
00-017 21 mars 2000	Délibération décidant un contrôle sur place
00-018 21 mars 2000	Délibération décidant un contrôle sur place
00-019 21 mars 2000	Délibération décidant un contrôle sur place
00-020. 21 mars 2000	Délibération décidant un contrôle sur place
00-021 30 mars 2000	Délibération concernant la mise en oeuvre par la direction générale de la comptabilité publique du traitement « GIR » ayant pour objet la gestion du compte unique du contribuable en matière d'impôts directs
00-022 30 mars 2000	Délibération portant avis sur un projet de décret présenté par le ministère de l'Agriculture relatif à la communication d'informations par les caisses de la mutualité sociale agricole aux commissions chargées d'établir les listes électorales pour les élections aux chambres d'agriculture
00-023 30 mars 2000	Délibération portant avis sur un projet de décret présenté par le secrétariat d'État à l'Outre-Mer relatif à la création d'un traitement automatisé nécessaire à la tenue du fichier général des électeurs inscrits en Nouvelle-Calédonie
00-024 27 avril 2000	Délibération décidant un contrôle sur place
00-025 27 avril 2000	Délibération décidant un contrôle sur place

Numéro Date	Date et objet
00-026 27 avril 2000	Délibération décidant un contrôle sur place
00-027 27 avril 2000	Délibération décidant un contrôle sur place
00-028 27 avril 2000	Délibération décidant un contrôle sur place
00-029 25 mai 2000	Délibération portant élection du vice-président de la Commission nationale de l'informatique et des libertés
00-030	*numéro non attribué*
00-031 25 mai 2000	Délibération portant avis sur le projet d'acte réglementaire présenté par le CREDOC et concernant la mise en œuvre d'une base de données statistiques dans le cadre de l'observatoire des entrées et sorties du dispositif RMI à Paris
00-032 8 juin 2000	Délibération décidant un contrôle sur place
00-033 8 juin 2000 (cf. p. 69)	Délibération relative à une demande de conseil présentée par le ministère de l'Emploi et de la Solidarité sur la mise en œuvre du numéro gratuit, le 114, destiné à lutter contre les discriminations raciales
00-034 8 juin 2000	Délibération relative à la modification des procédures de télétransmission des déclarations fiscales professionnelles
00-035 20 juin 2000 (cf. p. 46)	Délibération portant dénonciation au Parquet de faits imputés à l'association spirituelle de l'Eglise de Scientologie d'Île-de-France

Numéro Date	Date et objet
00-036 4 juillet 2000	Délibération relative à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 et à un projet d'arrêté concernant le transfert à la commission d'indemnisation des victimes de spoliations du fichier constitué par la mission d'étude sur la spoliation des personnes considérées comme juives
00-037 4 juillet 2000	Délibération portant avis sur un projet d'arrêté modifiant l'arrêté du 18 juin 1999 présenté par le ministère de la Justice relatif à un modèle-type de traitement concernant le suivi des affaires pénales du Parquet général des cours d'appel
00-038 4 juillet 2000	Délibération portant avis sur l'utilisation, par l'INSEE, du fichier de la taxe d'habitation en vue des prochains recensements de population
00-039 4 juillet 2000	Délibération portant avis sur la mise en place, par l'INSEE, d'un répertoire des immeubles localisés (R.I.L.)
00-040 4 juillet 2000	Délibération relative à une demande d'avis sur un projet de décret relatif à la transposition en droit français des directives 97/66/CE et 98/10/CE et modifiant le code des postes et télécommunications
00-041 21 septembre 2000	Délibération portant avis sur un projet de disposition législative relative à la création d'un répertoire national des retraites et des pensions et d'un échantillon inter régimes de cotisants
00-042 21 septembre 2000	Délibération relative à un projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 au fichier mis en oeuvre par la Commission pour l'indemnisation des victimes de spoliations
00-043 3 octobre 2000	Délibération concernant l'informatisation de la gestion par la direction générale des Impôts de la taxe annuelle sur les logements vacants
00-044 3 octobre 2000	Délibération relative à la modification du traitement « ILIAD » de la direction générale des Impôts, et notamment à la mise en place du dossier « 2004 Informatique »

Numéro Date	Date et objet
00-045 3 octobre 2000 (cf. p. *55)*	Délibération portant avis sur un projet de décret modifiant les articles R 11-1, R 11-2, R 11-3 et R 11-4 du code de la santé publique issus du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire
00-046 12 octobre 2000	Délibération portant sur la demande d'avis présentée par l'INSEE relative à une enquête sur les déplacements et moyens de communication des ménages de la région stéphanoise
00-047 12 octobre 2000	Délibération décidant un contrôle sur place
00-048 12 octobre 2000	Délibération décidant un contrôle sur place
00-049 12 octobre 2000	Délibération décidant un contrôle sur place
00-050 12 octobre 2000	Délibération décidant un contrôle sur place
00-051 12 octobre 2000	Délibération décidant un contrôle sur place
00-052 12 octobre 2000	Délibération décidant un contrôle sur place
00-053 26 octobre 2000	Délibération concernant l'informatisation de la gestion par la direction générale des Impôts de la taxe annuelle sur les logements vacants
00-054 12 octobre 2000	Délibération décidant un contrôle sur place

Numéro Date	Date et objet
00-055 16 novembre 2000	Délibération portant sur la demande d'avis présentée par l'INSEE relative à la mise en oeuvre d'une enquête dénommée « Sans domicile 2001 »
00-056 16 novembre 2000 (cf. p. 118)	Délibération portant avis sur un projet d'arrêté présenté par le ministre de l'Education nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès, par la reconnaissance des empreintes digitales de certains personnels de l'Éducation nationale, pour certains locaux de la cité académique de Lille
00-057 16 novembre 2000 (cf. p. 113)	Délibération portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture
00-058 16 novembre 2000	Délibération portant avis sur un projet de décret présenté par le secrétariat d'État à l'Outre-mer relatif à la création d'un traitement automatisé nécessaire à la tenue du fichier général des électeurs inscrits à Mayotte
00-059 30 novembre 2000	Délibération portant avis sur un projet d'arrêté modifiant l'arrêté du 28 avril 1993 présenté par le ministère de la Justice relatif à un traitement national ayant pour finalité le suivi des mesures éducatives et de l'activité des services du secteur public de la protection judiciaire de la jeunesse
00-060 30 novembre 2000	Délibération décidant un contrôle sur place
00-061 30 novembre 2000	Délibération décidant un contrôle sur place
00-062 30 novembre 2000	Délibération décidant un contrôle sur place
00-063 30 novembre 2000 (cf. p. 63)	Délibération portant avis sur le projet de délibération du conseil d'administration du SNATEM concernant la mise en œuvre du traitement AGATE de gestion des appels reçus

Numéro Date	Date et objet
00-064 19 décembre 2000 (cf. p. 89)	Délibération relative à un projet de décret en Conseil d'État portant création du « système de traitement des infractions constatées » (STIC) et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978

Annexe 5

Délibérations adoptées en 2000, non publiées dans les chapitres du rapport

Délibération n° 00-001 du 13 janvier 2000 portant autorisation de mise en œuvre par le Comité médical paritaire local des médecins généralistes de Paris d'un traitement de données personnelles de santé ayant pour objet l'évaluation des pratiques médicales de prescription dans la rhino-pharyngite de l'enfant.

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 loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique aux fichiers et aux libertés et notamment son chapitre V ter ;

Vu le décret n° 78774 du 17 juillet 1978 modifié et notamment son chapitre IV ;

Vu la demande d'autorisation présentée par le Comité médical paritaire local des médecins généralistes de Paris ;

Après avoir entendu Monsieur Raymond Forni en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que, conformément à l'article 40-12 de la loi du 6 janvier 1978 modifiée, le Comité médical paritaire local des médecins généralistes de Paris a saisi la Commission d'une demande d'autorisation portant sur la collecte de données à des fins d'évaluation des pratiques médicales de prescription dans la rhino-pharyngite de l'enfant de 6 mois à 6 ans ;

Considérant que les données collectées auprès de médecins généralistes volontaires sont relatives à la date de naissance, au sexe, à l'environnement familial, à la catégorie socioprofessionnelle des parents, au mode de vie, à la prise en charge administrative et au diagnostic et à la prescription effectuée, à l'exclusion du nom, du prénom et du numéro de sécurité sociale ;

Considérant que l'article 40-13 de la loi du 6 janvier 1978, issue de l'article 41 de la loi du 27 juillet 1999, prévoit que les données issues des dossiers médicaux détenus dans le cadre de l'exercice libéral des professions de santé sont librement communicables dès lors que les données sont présentées sous forme de statistiques agrégées ou constituées de telle sorte que les personnes concernées ne puissent être identifiées ; que le deuxième alinéa de cet article prévoit que des données issues de ces systèmes ne remplissant pas les conditions prévues par le premier alinéa peuvent encore être communiquées sur autorisation de la CNIL ; que, dans ce cas, il incombe à la CNIL de vérifier « les garanties présentées par le demandeur pour l'application des présentes dispositions et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social », de « s'assurer de la nécessité de recourir à des données personnelles et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques de soins et de prévention » ; qu'il revient également à la Commission de déterminer la durée

de conservation des données et d'apprécier les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi ;

Considérant qu'il appartiendra au service médical de la Caisse primaire d'assurance maladie de Paris de procéder au traitement des données ainsi recueillies afin d'établir des tableaux anonymes reprenant la prescription effectuée et son analyse au regard des références médicales opposables ; qu'aucun contrôle ne sera réalisé auprès des médecins concernés ;

Considérant que les résultats globaux ne permettant en aucun cas d'identifier la personne seront diffusés à tous les médecins généralistes ayant participé et à l'ensemble de la profession, sous la responsabilité du Comité médical paritaire ;

Considérant que le traitement informatique sera réalisé sous la responsabilité du médecin du service médical de la CPAM de Paris ; que l'accès à l'application sera protégé par des procédures de mots de passe individuels et qu'une journalisation des connexions sera mise en œuvre, de sorte que trace soit conservée de tout accès aux informations ;

Considérant que le président du Comité médical paritaire local des médecins généralistes de Paris s'engage ainsi que le service médical de la CPAM de Paris :
— à n'utiliser les fichiers qu'à des fins d'analyse comparative des prescriptions ;
— à respecter et à faire respecter le secret des informations cédées par toutes les personnes susceptibles de travailler sur ces données, ces personnes étant astreintes par écrit au secret professionnel ;
— à prendre toutes précautions utiles afin de préserver la sécurité des informations ainsi transmises et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ;
— à ne pas rétrocéder ou divulguer à des tiers les informations fournies sous quelque forme que ce soit ;
— à ne pas procéder à des rapprochements, interconnexions, mises en relation, appariements avec tout fichier de données directement ou indirectement nominatives ou toute information susceptible de révéler l'identité d'une personne ou/et son état de santé ;
— à ne pas utiliser de façon détournée les informations transmises, notamment à des fins de recherche ou d'identification des personnes ;

Considérant que l'architecture technique présentée et les engagements pris permettent de considérer que les garanties de sécurité sont sérieuses et de qualité ;

Considérant que le Comité médical paritaire local des médecins généralistes envisage de conserver les données transmises pendant deux ans afin de disposer du temps nécessaire, compte tenu de son mode de fonctionnement paritaire, pour procéder aux analyses susvisées ; que cette durée paraît satisfaisante ;

Considérant que les données collectées sont pertinentes au regard de la finalité de l'évaluation envisagée ;

Autorise le Comité médical paritaire des médecins généralistes de Paris à mettre en œuvre un traitement de données personnelles à des fins d'évaluation des pratiques de prescription dans le domaine de la rhino-pharyngite de l'enfant de 6 mois à 6 ans.

Délibération n° 00-002 du 13 janvier 2000 portant autorisation de mise en œuvre par l'Agence régionale de l'hospitalisation d'Île-de-France d'un traitement de données personnelles de santé à des fins d'évaluation des pratiques de soins en urgence face à un infarctus du myocarde.

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 loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique aux fichiers et aux libertés et notamment son chapitre V ter ;

Vu le décret n° 78774 du 17 juillet 1978 modifié et notamment son chapitre IV ;

Vu la demande d'autorisation présentée par l'Agence régionale de l'hospitalisation d'Ile-de-France ;

Après avoir entendu Monsieur Raymond Forni en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que, conformément à l'article 40-12 de la loi du 6 janvier 1978 modifiée, l'Agence régionale de l'hospitalisation d'Île-de-France (ARH) a saisi la Commission d'une demande d'autorisation portant sur une évaluation de la prise en charge initiale de l'infarctus du myocarde à travers l'activité des services d'aide médicale d'urgence et des services médicaux d'urgence et de réanimation ;

Considérant que les services d'urgence hospitaliers communiqueront par minitel à l'ARH les données suivantes : les trois premières lettres du nom, deux premières lettres du prénom, sexe, date de naissance, données cliniques relatives à la prise en charge précoce de l'infarctus du myocarde et indication de l'établissement où aura été orienté le patient ;

Considérant que l'article 40-13 de la loi du 6 janvier 1978, issue de l'article 41 de la loi du 27 juillet 1999, prévoit que les données issues des systèmes d'informations hospitaliers visés à l'article L 710-6 du code de la santé publique, sont librement communicables dès lors que les données sont présentées sous forme de statistiques agrégées ou constituées de telle sorte que les personnes concernées ne puissent être identifiées ; que le deuxième alinéa de cet article prévoit que des données issues de ces systèmes ne remplissant pas les conditions prévues par le premier alinéa, peuvent encore être communiquées sur autorisation de la CNIL ; que, dans ce cas, il incombe à la CNIL de vérifier « les garanties présentées par le demandeur pour l'application des présentes dispositions et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social », de « s'assurer de la nécessité de recourir à des données personnelles et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques de soins et de prévention » ; qu'il revient également à la Commission de déterminer la durée de conservation des données et d'apprécier les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi ;

Considérant que, d'une part, l'ARH d'Île-de-France effectuera des analyses statistiques sur les choix des techniques retenues lors des soins d'urgence et, d'autre part, des analyses exploratoires permettant d'obtenir, au vu de la conduite thérapeutique réalisée, une classification en fonction de facteurs de risque pertinents ; que les rapports établis ne permettront en aucune façon d'identifier la personne ;

Considérant que le traitement informatique sera réalisé sous la responsabilité du médecin responsable du schéma régional d'organisation sanitaire de cardiologie en Île-de-France et qu'il aura seul accès à l'ensemble des données transmises ; que l'accès à l'application sera protégé par des procédures de mots de passe individuels et qu'une journalisation des connexions sera mise en œuvre, de sorte que trace soit conservée de tout accès aux informations ;

Considérant que le responsable du projet à l'ARH d'Ile-de-France s'engage ainsi que ses collaborateurs :
— à n'utiliser les fichiers qu'à des fins d'analyse comparative de l'activité de soins ;
— à respecter et à faire respecter le secret des informations cédées par tou tes les personnes susceptibles de travailler sur ces données, ces personnes étant astreintes par écrit au secret professionnel ;
— à prendre toutes précautions utiles afin de préserver la sécurité des infor mations ainsi transmises et notamment d'empêcher qu'elles ne soient défor mées, endommagées ou communiquées à des tiers non autorisés ;
— à ne pas rétrocéder ou divulguer à des tiers les informations fournies sous quelque forme que ce soit ;
— à ne pas procéder à des rapprochements, interconnexions, mises en rela tion, appariements avec tout fichier de données directement ou indirecte ment nominatives ou toute information susceptible de révéler l'identité d'une personne ou/et son état de santé ;
— à ne pas utiliser de façon détournée les informations transmises, notam ment à des fins de recherche ou d'identification des personnes ;

Considérant que l'architecture technique présentée et les engagements pris permettent de considérer que les garanties de sécurité sont sérieuses et de qualité ;

Considérant que l'Agence régionale d'hospitalisation d'Île-de-France envisage de conserver les données qui lui seraient transmises pendant une durée de cinq ans afin de pouvoir efficacement évaluer des pratiques de soins à visée épidémiologique ; que cette durée est jugée satisfaisante ;

Considérant que la transmission à l'Agence régionale de l'hospitalisation d'Ile-de-France des trois premières lettres du nom et des deux premières lettres du prénom est présentée comme ayant pour objet de faciliter la validation des données auprès des services d'urgence ; que le recours à ces données identifiantes paraît excessif, au sens de l'article 5 de la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe, dans la mesure où cette validation pourrait reposer sur l'attribution d'un numéro d'ordre aux informations communiquées par les services d'urgence qui conserveraient la correspondance avec l'identité des patients ;

Considérant que l'Agence régionale de l'hospitalisation d'Île-de-France ne sera destinataire que des numéros ainsi attribués à l'exclusion de toute donnée d'identification ;

Autorise l'Agence régionale de l'hospitalisation d'Ile-de-France à mettre en oeuvre un traitement de données personnelles de santé à des fins d'évaluation des pratiques de soins en urgence face à un infarctus du myocarde, sous réserve de substituer, préalablement à la transmission des informations à l'ARH, un numéro aux trois premières lettres du nom et deux premières lettres du prénom.

Délibération n° 00-003 du 13 janvier 2000 portant autorisation de mise en œuvre par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins.

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 loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique aux fichiers et aux libertés et notamment son chapitre V ter ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié et notamment son chapitre IV ;

Vu la demande d'autorisation présentée par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif ; Après avoir entendu Monsieur Raymond Forni en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que, conformément à l'article 40-12 de la loi du 6 janvier 1978 modifiée, la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif (FEHAP) a saisi la Commission d'une demande d'autorisation portant sur la communication, à des fins de traitements d'analyse statistique de l'activité de soins, d'une copie informatique, établissement par établissement, des résumés de sortie anonymes et des résumés hebdomadaires anonymes détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1998 par les établissements de santé publics et privés participant ou ne participant pas au service public ;

Considérant qu'en application des articles L 710-6 et L 710-7 du Code de la Santé Publique, les praticiens exerçant dans les établissements de santé publics et privés sont tenus de communiquer les informations médicales nominatives nécessaires à l'analyse de leur activité au médecin responsable du département d'information médicale au sein de chaque établissement ; qu'il appartient à ce dernier de traiter ces informations et de les transmettre, sous forme de résumés de sortie anonymes (RSA) pour le court séjour ou de résumés hebdomadaires anonymes (RHA) pour le moyen et long séjour à la direction de l'établissement ainsi qu'aux DRASS, Caisses régionales d'assurance maladie et au ministère de l'Emploi et de la Solidarité qui fait procéder à leur exploitation statistique, dans le cadre du Programme de Médicalisation des Systèmes d'Information PMSI — système statistique d'évaluation de l'activité hospitalière utilisé en particulier pour le calcul des budgets hospitaliers ;

Considérant que les résumés de sortie anonymes (RSA) indiquent, pour chaque séjour hospitalier, l'établissement où le patient a été hospitalisé, son sexe, son âge et le code géographique de résidence, la durée de séjour, le ou les codes des pathologies diagnostiquées, le ou les codes des actes pratiqués ; qu'ainsi, l'identité des patients n'est en aucun cas communiquée ; que les résumés hebdomadaires anonymes (RHA), établis dans le cadre du PMSI moyen et long séjour, indiquent pour chaque séjour hospitalier l'établissement où le patient a été hospitalisé, son sexe, son âge, le code géographique de résidence, la durée du séjour en semaines, la finalité principale de la prise en charge, le ou les diagnostics pratiqués, le ou les codes pratiqués ;

Considérant que l'article 40-13 de la loi du 6 janvier 1978, issu de l'article 41 de la loi du 27 juillet 1999, prévoit que les données issues des systèmes d'informations visés à l'article L 710-6 du code de la santé publique, parmi lesquels figure le PMSI, sont librement communicables dès lors que les données sont présentées sous forme de statistiques agrégées ou constituées de telle sorte que les personnes concernées ne puissent être identifiées ; que le deuxième alinéa de cet article prévoit que des données issues de ces systèmes ne remplissant pas les conditions prévues par le premier alinéa peuvent encore être communiquées sur autorisation de la CNIL ; que, dans ce cas, il incombe à la CNIL de vérifier « les garanties présentées par le demandeur pour l'application des présentes dispositions et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social », de « s'assurer de la nécessité de recourir à des données personnelles et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques de soins et de prévention » ; qu'il revient également à la Commission de déterminer la durée de conservation des données et d'apprécier les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi ;

Considérant que la Fédération sollicite l'obtention d'informations issues des « résumés de sortie anonymes » et des « résumés hebdomadaires anonymes », pour réaliser une analyse de l'activité hospitalière privée participant et/ou ne participant pas au service public, dans la perspective d'effectuer des analyses comparatives, d'élaborer un classement des séjours plus opérationnel que celui retenu actuellement par le PMSI et de préparer une « classification à la pathologie » en comparant des séjours classés de façon identique mais dont les coûts peuvent s'avérer très différents selon les établissements ;

Considérant qu'il y a lieu de rappeler, d'une part, que les « résumés de sortie anonymes » et les « résumés hebdomadaires anonymes » comportent des données individuelles dont l'exploitation informatique ne permet pas, à elles seules, d'identifier les patients concernés ; que toutefois ces données sont susceptibles, dès lors qu'il serait procédé à leur rapprochement avec d'autres informations ou fichiers comportant l'identité de personnes hospitalisées, de déterminer, par recoupement, le motif d'hospitalisation de celles-ci ; qu'une telle identification de la personne à laquelle les données figurant dans le « résumé de sortie anonyme » ou dans le « résumé hebdomadaire anonyme » se rapportent, suppose cependant de connaître à la fois l'identité de la personne en cause et l'établissement dans lequel elle a suivi des soins ; qu'à défaut de ces deux informations, prises ensemble, aucune identification n'est possible, fut-ce par recoupement avec d'autres données ;

Considérant, d'autre part que la volonté pour la FEHAP de disposer de données lui permettant d'évaluer et d'améliorer l'activité de soins offerts par ses établissements adhérents constitue un objectif légitime dès lors qu'il ne résulterait de la communication de telles informations, des conditions de leur exploitation et des modalités de leur diffusion, aucune atteinte directe ou indirecte à la vie privée des personnes concernées et aucune possibilité d'identifier les patients en cause ou les pathologies dont ils souffrent ; qu'il importe à cet égard que toutes précautions soient prises non seulement pour garantir la confidentialité des données ainsi transmises et éviter leur divulgation mais également pour empêcher que ces données ne puissent être utilisées par quiconque à des fins de recherche ou d'identification des personnes ;

Considérant que c'est au regard de ces deux observations qu'il revient à la CNIL d'examiner, dans le respect des dispositions légales, la demande d'autorisation dont elle est saisie ;

Considérant que la Fédération prévoit que l'ensemble des traitements informatiques soit réalisé, sous la responsabilité du président, au siège de la Fédération, sur des ordinateurs fonctionnant en réseau fermé, accessibles uniquement à l'équipe chargée des travaux de recherche, soit trois personnes ; que l'accès à l'application sera protégé par des procédures de mots de passe individuels et qu'une journalisation des connexions sera mise en oeuvre, de sorte que trace soit conservée de tout accès aux informations ;

Considérant que le président de la Fédération s'engage ainsi que ses collaborateurs :
— à n'utiliser les fichiers qu'à des fins d'analyse comparative de l'activité de soins ;
— à respecter et à faire respecter le secret des informations cédées par tou tes les personnes susceptibles de travailler sur ces données, ces personnes étant astreintes par écrit au secret professionnel ;
— à prendre toutes précautions utiles afin de préserver la sécurité des infor mations ainsi transmises et notamment d'empêcher qu'elles ne soient défor mées, endommagées ou communiquées à des tiers non autorisés ;
— à ne pas rétrocéder ou divulguer à des tiers les informations fournies sous quelque forme que ce soit ;
— à ne pas procéder à des rapprochements, interconnexions, mises en rela tion, appariements avec tout fichier de données directement ou indirecte ment nominatives ou toute information susceptible de révéler l'identité d'une personne ou/et son état de santé ;
— à ne pas utiliser de façon détournée les informations transmises, notam ment à des fins de recherche ou d'identification des personnes ;

Considérant que l'architecture technique présentée et les engagements pris permettent de considérer que les garanties de sécurité sont sérieuses et de qualité ;

Considérant que président de la FEHAP s'engage à ce que les informations tirées des exploitations de fichiers et susceptibles d'être diffusées se présentent uniquement sous la forme de statistiques agrégées de telle sorte que les personnes ne puissent être identifiées ;

Considérant que la Fédération envisage de conserver les données qui lui seraient transmises pendant une durée de trois ans afin de pouvoir notamment

entreprendre des études de comparaison avec les bases de données des années ultérieures ;

Considérant qu'au regard de la finalité poursuivie par le traitement, la durée de conservation doit être limitée au temps nécessaire à la réalisation des traitements en vue de la diffusion des résultats obtenus aux adhérents ; qu'à cet égard, la durée de trois ans est jugée satisfaisante ;

Considérant que c'est au regard de ces garanties préalables que doit être appréciée la nécessité pour le demandeur, de disposer des données sollicitées ;

Considérant qu'au regard de la finalité d'analyse globale des pratiques de soins, le recueil, sous une forme détaillée, de l'âge précis des patients n'est pas utile ; qu'il y a lieu de prévoir sur ce point que seule une tranche d'âge de cinq ans en cinq ans sera mise à la disposition du demandeur ; que, s'agissant des nouveaux-nés, la transmission de l'indication d'un âge inférieur à un an est suffisante ;

Considérant que la CNIL prend acte de ce que la Fédération ne sollicite que la communication du département de résidence et non du code géographique du lieu de résidence des patients ; qu'en outre, elle ne souhaite pas obtenir l'indication du décès dans la rubrique sur le mode de sortie, ni du mois de sortie ;

Autorise la Fédération des établissements et d'assistance privés à but non lucratif (FEHAP) à obtenir communication, à des fins de traitements d'analyse statistique de l'activité de soins, d'une copie informatique, établissement par établissement, des informations issues des résumés de sortie anonymes et des résumés hebdomadaires anonymes détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1998 par les établissements de santé publics et privés participant ou ne participant pas au service public, sous réserve que l'âge précis des patients soit remplacé par une indication de l'âge par tranche de cinq ans et que pour les nouveaux nés, seule soit communiquée l'indication d'un âge inférieur à un an.

Délibération n° 00-005 du 27 janvier 2000 portant avis sur un projet d'acte réglementaire présenté par l'UNEDIC portant création d'un fichier national des ASSEDIC.

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 la loi n° 79-18 du 3 janvier 1979 sur les archives ;

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

Vu le décret 87-1025 du 17 décembre 1987 modifié, relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage ;

Après avoir entendu Monsieur Hubert Bouchet, vice-président délégué, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que l'UNEDIC a déposé une demande d'avis relative à un traitement automatisé d'informations nominatives ayant pour finalité la gestion d'un fichier national statistique des allocataires ;

Considérant que l'UNEDIC souhaite disposer d'un outil statistique dénommé « Fichier National des Allocataires » FNA, dont la finalité est d'effectuer des suivis spécifiques et historiques des populations dans l'optique d'une analyse du marché du travail, d'effectuer des simulations sur les conséquences des changements réglementaires et d'évaluer les nouveaux dispositifs réglementaires ; que ce traitement n'est ni destiné à gérer les indemnisations ni destiné à contrôler les personnes bénéficiaires du régime d'assurance chômage ;

Considérant que ce traitement englobe les allocataires percevant une allocation gérée par le régime d'assurance chômage ainsi que les personnes inscrites comme demandeurs d'emploi et potentiellement allocataires ;

Considérant que ce traitement est constitué des informations issues des fichiers opérationnels des ASSEDIC concernant les personnes ayant fait l'objet d'une inscription, d'une liquidation, d'une radiation ou de toute autre modification ; que chaque mouvement est inscrit dans le FNA au titre de son bénéficiaire ;

Considérant que les informations enregistrées seront : le NIR, le département et la commune de résidence, les caractéristiques de la demande d'emploi (date d'inscription à l'ANPE / ASSEDIC), le code ROME, le métier recherché, le diplôme enseignement général et technique, les caractéristiques de la demande d'allocation et les caractéristiques des droits ouverts et des périodes d'indemnisation ;

Considérant que le traitement ne comporte pas les nom, prénom et adresse des personnes ; que toutefois, le numéro d'inscription ASSEDIC et le NIR lui confèrent un caractère indirectement nominatif ;

Considérant que le FNA permet de produire des fichiers et des échantillons statistiques à destination des utilisateurs de la direction des études statistiques de l'UNEDIC par requête spécifique ;

Considérant que les autres destinataires des informations habilités à connaître des résultats des traitements statistiques, exclusivement sous forme de tableaux statistiques, sont les partenaires sociaux participant à la gestion du régime d'assurance chômage, la direction de l'UNEDIC, les ASSEDIC et la DARES ;

Considérant que les informations sont transmises sous la forme d'échantillon statistique et de tableaux statistiques ; que les tableaux et les échantillons statistiques transmis ne comportent pas le NIR des personnes ;

Considérant que le fichier sera constitué de deux parties, l'une active et l'autre archivée ; que les informations conservées dans la partie active sont relatives aux droits à allocation ou aux inscriptions des demandeurs non indemnisés ayant moins de trois ans ;

Considérant qu'au-delà de ce délai de trois ans, les informations sont transférées dans la partie archive ; que toutefois ces informations pourront faire l'objet ponctuellement de nouveaux traitements statistiques ;

Considérant que les informations ne sauraient être conservées, même sous forme indirectement nominative, de façon illimitée ;

Considérant que la directive européenne du 24 octobre 1995 prévoit des dispositions particulières relatives aux traitements statistiques ; que le projet de loi relatif aux relations des citoyens avec l'administration, actuellement en cours de discussion devant le Parlement, s'efforce de mieux concilier les dispositions de la loi du 6 janvier 1978 avec celles de la loi du 3 janvier 1979 sur les archives, aux termes desquelles toute information publique est imprescriptible et peut être versée et conservée par les archives au-delà de sa durée d'usage à des fins historiques ou statistiques ;

Considérant que l'information des personnes concernées sur la mise en œuvre de ce traitement statistique sera effectuée à l'aide de l'imprimé unique d'inscription par lequel les personnes s'inscrivent auprès de l'ASSEDIC ; qu'il convient de prévoir une information spécifique des personnes d'ores et déjà indemnisées par le biais des envois de DSM ainsi que l'affichage de l'acte réglementaire portant création du traitement dans les locaux d'accueil des antennes ASSEDIC ;

Émet un avis favorable sur le projet de délibération de l'UNEDIC portant création du FNA sous réserve que les informations archivées ne soient conservées par l'UNEDIC à des fins de traitements statistiques ultérieurs que pendant une durée de dix ans.

Délibération n° 00-006 du 27 janvier 2000 portant avis sur un traitement de l'UNEDIC ayant pour finalité la gestion des opérations administratives et techniques relatives à l'inscription des demandeurs d'emploi par les ASSEDIC.

(Demande d'avis n° 660918)

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

Vu le décret 87-1025 du 17 décembre 1987 modifié, relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage ;

Vu l'article L 311-8 du code du travail ;

Vu la convention du 4 juillet 1996 relative à la gestion des opérations d'inscription sur la liste des demandeurs d'emploi agréé par un arrêté du 13 mars 1997 ;

Après avoir entendu Monsieur Hubert BOUCHET, vice-président délégué, en son rapport et Madame Charlotte-Marie PITRAT, commissaire du gouvernement, en ses observations ;

Considérant que la convention du 4 juillet 1996 signée entre l'ANPE et l'UNEDIC a organisé le transfert de l'inscription des demandeurs d'emploi des agences locales pour l'emploi vers les ASSEDIC et précisé les conditions de ce transfert ; que depuis le 1er janvier 1998 les opérations administratives et techniques liées à l'inscription des demandeurs d'emploi et au versement des revenus de remplacement sont effectuées auprès et par les ASSEDIC, l'ANPE conservant la maîtrise des opérations liées au placement, au contrôle de la recherche d'emploi et aux éventuelles radiations ;

Considérant que les ASSEDIC sont chargées d'accueillir les demandeurs d'emploi et de les informer de leurs droits qu'ils soient ou non susceptibles d'obtenir des allocations chômage ; que l'inscription est réalisée au moyen d'un formulaire commun entre l'ANPE et les ASSEDIC ;

Considérant que les informations recueillies sont enregistrées dans le fichier commun ANPE / ASSEDIC dénommé Gide I Bis ; que les informations recueillies à l'occasion de l'inscription sont le nom de la personne, le prénom, la date de naissance, le numéro de sécurité sociale, la nationalité et le titre de séjour et/ou de travail, l'adresse, le numéro de téléphone, le motif de l'inscription, le type d'emploi recherché, la disponibilité de la personne, si elle bénéficie du RMI, si elle est travailleur handicapé, si elle bénéficie d'une pension d'invalidité, d'une rente pour accident du travail, si elle est mutilé de guerre, si elle a déjà été inscrite comme demandeur d'emploi, le détail de toutes les périodes d'emploi des quatre dernières années, les indemnités liées à la rupture du contrat de travail et si la personne était dirigeant d'entreprise, associé, commerçant, artisan ;

Considérant que ces informations permettent d'assurer le calcul et le versement des revenus de remplacement et de classer le demandeur d'emploi dans l'une des six catégories destinée au recensement des demandeurs d'emploi selon leurs disponibilités afin de permettre à l'ANPE d'ajuster ses offres et ses prestations ;

Considérant que l'inscription prend effet à la date de présentation de la personne dès lors que toutes les pièces justificatives ont été fournies ; que s'il s'agit d'une réinscription le demandeur d'emploi n'a pas besoin de se présenter physiquement ; que l'ASSEDIC fournit alors au demandeur d'emploi une attestation d'inscription sous la forme d'une carte de demandeur d'emploi et invite la personne à se rendre dans son agence locale pour l'emploi (ALE) pour un « premier entretien de recherche d'emploi » qui doit avoir lieu dans les quatre semaines suivant l'inscription ; que si le demandeur d'emploi ne se présente pas pour cet entretien sans motif légitime, il est alors radié.

Considérant qu'il a été constaté au cours de la visite sur place auprès d'une antenne ASSEDIC que le demandeur d'emploi se voyait remettre un livret lui expliquant toutes les démarches qu'il aurait à accomplir et l'informant de son droit d'accès et de rectification ;

Considérant que l'inscription comme demandeur d'emploi doit être renouvelée tous les mois au moyen d'une déclaration mensuelle de situation (DSM) récapitulant les éventuelles périodes de travail, de stage, d'arrêt maladie, demandant si la personne est toujours à la recherche d'un emploi et servant à calculer le montant de l'allocation qui sera versée à l'allocataire le mois suivant ;

Considérant que l'actualisation de la situation peut également être réalisée par téléphone, par minitel et bientôt à l'aide de bornes interactives situées dans les antennes ASSEDIC ; que les réponses fournies par la téléactualisation doivent être validées par l'allocataire ;

Considérant que le document d'actualisation envoyé chaque mois aux allocataires comporte systématiquement le code personnel de la personne lui permettant d'effectuer l'actualisation par téléphone, minitel ou borne interactive ; qu'il conviendrait que ce code fasse l'objet d'un envoi séparé afin de garantir sa confidentialité et qu'il ne soit plus porté systématiquement sur les documents reçus par le demandeur d'emploi.

Considérant que le projet de mise en place d'une carte à mémoire du demandeur d'emploi devra faire l'objet d'une demande d'avis auprès de la Commission ;

Considérant que les informations relatives à l'allocataire sont conservées pendant une durée de trois ans à l'issue de l'épuisement des droits ; qu'une telle durée destinée à assurer la pérennité des droits des allocataires est justifiée ;

Considérant que le livret remis aux allocataires au moment de leur inscription comporte de nombreux documents sur lesquels figurent les mentions de l'article 27 de la loi du 6 janvier 1978 ; que les supports servant à réaliser la déclaration mensuelle de situation adressée chaque mois aux allocataires comportent également ces mentions et que chaque antenne ASSEDIC affichera dans les locaux d'accueil l'acte réglementaire portant transfert de l'inscription des demandeurs d'emploi ;

Considérant que la Commission qui avait relevé que les allocataires avaient des difficultés pour exercer leur droit d'accès aux informations les concernant dans un délai raisonnable prend acte qu'à la suite des visites de vérification qui ont eu lieu au printemps, les demandes de droit d'accès pour lesquelles la Commission intervient à l'appui des allocataires sont satisfaites très rapidement ;

Considérant que la modification du régime de la preuve permettra aux ASSEDIC d'utiliser les documents d'actualisation quel que soit leur support (papier ou image scanérisée) et leur mode de réalisation (téléphone, minitel ou borne interactive) ; que les documents d'actualisation devront impérativement identifier la personne dont ils émanent et devront être conservés de façon à en garantir l'intégrité ;

Prend acte des améliorations apportées par les ASSEDIC à l'accueil des allocataires et l'exercice de leur droit d'accès.

Émet un avis favorable au projet d'acte réglementaire relatif à la mise en œuvre de la gestion des opérations d'inscription sur la liste des demandeurs d'emploi par les ASSEDIC.

Délibération n° 00-007 du 27 janvier 2000 portant avis sur le projet de modification du décret 87-1025 du 17 décembre 1987 relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage.

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 351-2 du code du travail ;

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

Vu le décret 87-1025 du 17 décembre 1987 modifié, relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage ;

Après avoir entendu Monsieur Hubert BOUCHET, vice-président délégué, en son rapport et Madame Charlotte-Marie PITRAT, commissaire du gouvernement, en ses observations ;

Considérant que le ministère de l'Emploi et de la Solidarité a saisi la Commission de deux projets de modification du décret 87-1025 du 17 décembre 1987 modifié, relatif à l'utilisation du répertoire national d'identification des personnes physiques par l'ANPE et les institutions gestionnaires du régime d'assurance chômage ;

Considérant que ces modifications ont pour objet d'ajouter un paragraphe 4 et un paragraphe 5 au décret précité ;

Considérant que le nouveau paragraphe 4 disposerait que l'UNEDIC est autorisé à collecter le NIR pour rassembler et traiter à des fins statistiques, des informations individuelles relatives à leurs allocataires ou aux demandeurs d'emploi les sollicitant en vue de percevoir tout revenu de remplacement géré par elles ;

Considérant que le fonctionnement du régime d'assurance chômage est tel que les identifiants ASSEDIC sont gérés par chaque CSIA (centre de service inter ASSEDIC, au nombre de 5) regroupant plusieurs régions ; que cette multiplicité des identifiants ainsi que leur construction a rendu nécessaire la création du répertoire national des allocataires ne comportant que les données d'identification, dont le NIR permettant de s'assurer en direct qu'une même personne n'est pas déjà inscrite pour la même période comme demandeur d'emploi dans une autre ASSEDIC ; que dans la mesure où le seul élément récurrent entre plusieurs périodes d'indemnisation et entre plusieurs inscriptions dans des régions éventuellement différentes est le NIR, son utilisation comme outil statistique est justifiée ;

Considérant que ce paragraphe a pour effet de permettre à l'UNEDIC d'utiliser le NIR comme outil statistique dans son fichier national des allocataires ; que ce traitement a fait l'objet d'un avis favorable de la Commission par la délibération n° 00-005 du 27 janvier 2000 ;

Considérant que le nouveau paragraphe 5 disposerait que les institutions gestionnaires du régime d'assurance chômage sont autorisées à consulter le répertoire national d'identification des personnes physiques afin d'obtenir ou de vérifier le numéro d'inscription au répertoire des demandeurs d'emploi indemnisés ou demandant à être indemnisés pour communiquer aux employeurs mentionnés à l'article L 351 -2 précité du code du travail assurant la charge et la gestion de l'allocation d'assurance, le NIR de leurs anciens salariés inscrits comme demandeurs d'emploi ;

Considérant que ce paragraphe permettrait la prise en compte par les services des ASSEDIC des agents non fonctionnaire de l'Etat et de ses établissements publics administratifs, des agents titulaires et non titulaires des collectivités territoriales, des agents statutaires et non statutaires des autres établissements publics administratifs ainsi que des agents non statutaires des groupements d'intérêt public tels qu'énumérés à l'article L 351-12 du code du travail ;

Considérant que ce projet de modification a pour objet de faire bénéficier les personnes ayant exercé un emploi pour un employeur public des prestations du régime d'assurance chômage au même titre et dans les mêmes conditions que les personnes ayant exercé un emploi pour un employeur du secteur privé et qu'il n'appelle pas d'observations particulières ;

Considérant que ce traitement a fait l'objet d'un avis favorable de la Commission par la délibération n° 00-006 du 27 janvier 2000 ;

Émet un avis favorable aux ajouts des paragraphes 4 et 5 au décret 87-1025 du 17 décembre 1987.

Délibération n° 00-008 du *17* janvier 2000 portant avis sur un projet d'arrêté du premier président de la Cour des comptes relatif à la création d'un traitement automatisé ayant pour finalité le contrôle des rémunérations versées à leur personnel par l'État et ses établissements publics.

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 des données à caractère personnel ;

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

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

Vu le code des juridictions financières ;

Vu le décret n° 85-199 du 11 février 1985 modifié relatif à la Cour des comptes ;

Vu le projet d'arrêté du Premier Président de la Cour des comptes relatif à la création d'un traitement, à la Cour des comptes, ayant pour finalité le contrôle des rémunérations versées à leur personnel par l'Etat et ses établissements publics ;

Après avoir entendu M. Gérard Gouzes en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ; Considérant que la Cour des comptes a saisi la Commission d'une demande d'avis relative à la création d'un traitement ayant pour finalité de permettre le contrôle des rémunérations versées à leur personnel par l'Etat et ses établissements publics ; qu'il sera procédé à l'exploitation des historiques des sommes payées ou retenues qui récapitulent les informations figurant sur les fiches de paye des personnels rémunérés par l'Etat, et que les comptables publics sont tenus de transmettre à la Cour des comptes ;

Considérant que ces informations étaient jusqu'à présent transmises à la Cour sur micro-fiches et seront désormais communiquées sur support informatique afin d'en permettre une exploitation plus aisée ;

Considérant que la Cour des comptes est habilitée, au titre de son pouvoir de contrôle juridictionnel sur les comptables publics, à obtenir communication de ces informations afin de contrôler la régularité du paiement des rémunérations des fonctionnaires et assimilés ;

Considérant en outre que l'examen des dispositions relatives aux pouvoirs d'investigation de la Cour fait apparaître que le législateur a souhaité lui reconnaître un accès très large aux informations détenues par les organismes et services placés sous son contrôle, qui est consubstantiel à ses missions de contrôle ; que l'article 18 du décret du 11 février 1985 précise que les rapporteurs de la Cour doivent notamment pouvoir demander la réalisation de traitements automatisés sur l'intégralité des fichiers informatisés de données nominatives des organismes contrôlés ;

Considérant que le projet d'arrêté prévoit que seront enregistrées dans le traitement les informations relatives à l'identité de la personne, son numéro de sécurité sociale, sa situation familiale dont le nombre d'enfants à charge, son statut au sein de la fonction publique, son service et son lieu d'affectation, ses fonctions, les services ordonnateurs et comptables chargés de sa rémunération, sa zone de résidence, le détail des rémunérations servies, des retenues effectuées ainsi que les charges salariales directement versées par l'administration employeur, telles qu'elles figurent dans les historiques des sommes payées ou retenues transmis à la Cour des comptes ; que le numéro de sécurité sociale des personnes, qui figure sur ces documents, ne sera pas utilisé dans le traitement comme critère de tri et que son utilisation demeurera accessoire ;

Considérant que le projet d'arrêté prévoit que les informations seront conservées pendant une durée de quatre ans ; qu'en effet l'article 16 du décret n° 69-366 du 11 avril 1969 précise que « La Cour des comptes est tenue de conserver les pièces justificatives qui lui sont produites pendant un délai de quatre années à partir de la clôture de l'exercice auquel se rattachent les pièces » ;

Considérant que le traitement sera mis en œuvre sur un micro-ordinateur unique, non connecté au réseau de la Cour des comptes, dans une pièce sécurisée ; qu'il ne sera accessible qu'aux magistrats, rapporteurs et assistants chargés, au sein de la Cour, du contrôle des rémunérations ;

Considérant que le droit d'accès des personnes concernées s'exercera en application de l'article 34 de la loi du 6 janvier 1978 auprès du secrétariat général de la Cour des comptes, sans préjudice de l'application des dispositions relatives à la communication des pièces justificatives détenues par la Cour ;

Émet, en conséquence, **un avis favorable** au projet d'arrêté présenté par le Premier Président de la Cour des comptes.

Délibération n° 00-009 du 27 janvier 2000 portant avis sur une demande d'avis du secrétaire d'État à l'Industrie relative à l'article 7 d'un avant-projet de loi portant diverses dispositions d'harmonisation communautaire (article destiné à compléter la transposition en droit français de la directive 97/66 concernant la protection des données à caractère personnel et la vie privée dans le secteur des télécommunications).

La Commission nationale de l'informatique et des libertés,

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 son application ;

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 directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ; Vu le code civil ; Vu le code des PetT ;

Vu l'article 7 de l'avant-projet de loi, transmis le 22 décembre 1999 pour avis par Monsieur Christian Pierret, secrétaire d'État à l'industrie, portant diverses dispositions d'harmonisation communautaire, destiné à compléter la transposition en droit français de la directive 97/66/CE ; Après avoir entendu Monsieur Marcel Pinet, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que l'article 7 de l'avant-projet de loi portant diverses dispositions d'harmonisation communautaire est destiné à compléter la transposition en droit français de la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications,

Sur les mesures de protection à l'égard des prospections directes non sollicitées auprès des abonnés aux réseaux de télécommunication réalisées au moyen d'automates d'appels ou de télécopieurs

Considérant que l'article 7 de l'avant-projet de loi pose le principe de l'interdiction du démarchage effectué au moyen d'un automate d'appels ou d'un télécopieur sans le consentement préalable des abonnés concernés ; que cet

article dispose dans un second alinéa que les opérateurs de télécommunications et leurs distributeurs permettent à chacun de leurs abonnés qui le souhaitent d'exprimer leur consentement à recevoir de tels appels au moment de la prise d'abonnement ou, ultérieurement à tout moment, et tiennent à la disposition de toute personne qui le leur demanderait la liste des abonnés ayant donné leur accord pour être prospecté de cette manière ;

Considérant qu'en ce qui concerne la prospection par automate d'appels, ce projet consacre la doctrine élaborée de longue date par la Commission ;

Considérant que s'agissant de la prospection par télécopieur, cet article renforce les garanties jusqu'à présent reconnues en France qui permettaient à toute personne, en s'inscrivant sur la liste « SAFRAN », de s'opposer à recevoir des documents de prospection par télécopie, mais qui autorisaient l'utilisation de ce moyen de prospection à l'égard de tous les abonnés s'étant abstenus d'entreprendre une telle démarche ; que compte tenu du grand nombre de plaintes et réclamations adressées à la Commission sur le sujet, il y a lieu de se féliciter de ce renforcement des garanties offertes aux abonnés ;

Considérant qu'en visant les « abonnés », le texte proposé garantit les droits susmentionnés à tous les titulaires de ligne, qu'il s'agisse de personnes physiques ou de personnes morales, ce qu'autorise assurément la directive 97/66/CE ;

Considérant cependant que le texte soumis à l'avis de la Commission, en ce qu'il ne vise que le « démarchage publicitaire », pourrait paraître ne pas réaliser la transposition imposée par le texte européen, qui vise la « prospection directe » ; que le texte proposé par le gouvernement devrait dès lors couvrir toutes les formes de prospection quelle qu'en soit la nature ; que serait ainsi couvert non seulement le démarchage publicitaire au sens strict mais également toutes les autres formes de démarchage (politique, associatif, religieux, caritatif, etc.) ;

Considérant dès lors que les mots « démarchage publicitaire » qui figurent au premier alinéa de l'article 7 nouveau, devraient être remplacés par les mots « prospection directe » ;

Sur la durée de conservation des données de facturation du détail des communications téléphoniques

Considérant que les dispositions de l'article 6 de la directive 97/66 relatif aux données de facturation des communications téléphoniques interdit aux opérateurs et à leurs distributeurs de conserver celles concernant le détail des communications au-delà de la période au cours de laquelle la facture peut être contestée ou des poursuites engagées pour en obtenir le paiement ;

Considérant, d'une part, que cette durée est, en France, variable selon l'opérateur ; qu'en particulier en application de l'article L 126 du code des PetT, France Télécom ne peut conserver ces données que pendant un an, tandis que des données de même nature peuvent être conservées pendant plus longtemps par les opérateurs qui ne sont pas tenus par les termes de cet article et qui relèvent des dispositions du code civil ; qu'en vertu du principe d'égalité de traitement qui doit s'appliquer à l'égard tant des opérateurs de télécommunications que des abonnés aux réseaux de télécommunications, il y a lieu d'unifier la durée de conservation en cause ; qu'à cet effet l'interven-

tion du législateur apparaît nécessaire et qu'il convient donc de compléter sur ce point l'avant-projet de loi soumis à la Commission ;

Considérant, d'autre part, que les données de facturation et de connexion touchent intimement à la vie privée des personnes ; qu'en effet elles révèlent l'intégralité des numéros appelés par un particulier, le moment exact de l'appel, ainsi que désormais, grâce aux nouvelles technologies, l'identification de la ligne appelée et, s'agissant des appels passés depuis un téléphone mobile, la localisation de l'appelant dans un rayon de quelques centaines de mètres ; que ces données peuvent en outre être accessibles, sur leur demande, pendant toute la période au cours de laquelle elles sont conservées, aux services de police ou à l'administration douanière notamment, en vertu des prérogatives que ces autorités tiennent des textes qui les régissent ;

Considérant que, compte tenu des incidences sur la vie privée des personnes de la durée pendant laquelle ces informations sont conservées, il y a lieu que cette durée concilie les exigences de protection de la vie privée et des libertés individuelles avec les légitimes besoins des autorités précitées pour l'exercice de leurs missions ;

Considérant qu'au regard de l'ensemble des éléments ci-dessus mentionnés comme des nécessités de gestion des opérateurs et compte tenu des termes actuels de l'article L 126 du code des PetT, une durée de conservation maximale d'un an des données de cette nature apparaît adaptée ; qu'en cas d'engagement d'une procédure contentieuse, ce délai ne devrait pas aller au-delà de l'intervention de la décision juridictionnelle définitive,

Émet un avis favorable à l'avant-projet de loi sous les deux réserves suivantes : 1 °/ dans l'article 7 de l'avant-projet de loi, les mots « démarchage publicitaire » sont à remplacer par les mots « prospection directe », 2°/ un article supplémentaire, ainsi rédigé, devrait être ajouté après l'article 7 :
« les données relatives à la facturation, appel par appel, des communications téléphoniques ainsi que l'ensemble des données de connexion ne peuvent être conservées par les opérateurs de télécommunication et leurs distributeurs, sur quelque support que ce soit, au-delà d'une durée d'un an, ou, en cas d'engagement d'une procédure contentieuse sur le recouvrement du montant des factures au-delà de l'intervention de la décision juridictionnelle définitive ».

Délibération 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.

La Commission nationale de l'informatique et des libertés,

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 le livre des procédures fiscales, notamment l'article R* 196-1 ; Vu trois projets d'arrêtés du ministre de l'Economie, des Finances et de l'Industrie concernant respectivement la transmission par voie électronique des éléments déclaratifs en matière d'impôt sur les revenus et portant conventions-types relatives à ces opérations, la modification consécutive de l'arrêté du 5 janvier 1990 relatif au traitement « FIP » et celle de l'arrêté du 5 janvier 1990 relatif au traitement « IR » ;

Après avoir entendu Monsieur Noël Chahid-Nouraï en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que le ministère de l'Économie et des Finances a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis relative à un projet de traitement de la direction générale des Impôts (DGI) dénommé « Télédéclaration IR », dont la finalité principale est de permettre aux contribuables qui le souhaitent de souscrire directement sur le réseau Internet leur déclaration de revenu global ainsi que leurs déclarations annexes, la télétransmission ne pouvant concerner toutefois les pièces justificatives qui ouvrent droit au bénéfice d'une réduction, lesquelles devront toujours être envoyées par courrier postal au centre des impôts mentionné sur le formulaire papier pré-identifié ;

Considérant que le projet de traitement ainsi soumis à l'examen de la Commission trouve son fondement dans la loi de finances rectificative pour 1999 qui étend aux déclarations fiscales des particuliers les dispositions de l'article 1649 quater B bis du code général des impôts autorisant la transmission par voie électronique des déclarations des entreprises, dans des conditions fixées par voie contractuelle ;

Considérant que, s'agissant des particuliers, les modalités de la télétransmission des déclarations sont également définies dans un contrat d'adhésion, lequel fixe les obligations des parties et détaille la procédure suivie, qui sera consultable sur le site web du ministère de l'Économie, des Finances et de l'Industrie et dont les clauses sont précisées dans le projet d'acte réglementaire soumis pour avis à la CNIL ;

Considérant qu'à la date à laquelle elle se trouve saisie de cette nouvelle téléprocédure, la Commission n'est plus en mesure de formuler utilement des suggestions de modification substantielle au dispositif technique envisagé ; qu'au surplus, une période d'acclimatation et d'essai est nécessaire à la mise au point définitive de ce dispositif ; qu'enfin, un certain nombre de réformes techniques et juridiques déjà programmées en ce qui concerne le recours aux procédés de signature électronique pourraient être de nature à influer sur ses modalités définitives ; qu'il y a lieu, dès lors et en premier lieu, de limiter la portée du présent avis à la mise en œuvre d'une expérimentation pendant la prochaine campagne, soit pendant une durée d'un an, et de

demander au ministère de l'Économie, des Finances et de l'Industrie de présenter, à l'issue de cette campagne, un bilan de l'opération assorti de perspectives d'aménagement visant à obtenir dès 2001 un renforcement des dispositifs de sécurité et de chiffrement, incluant notamment la mise en place d'un procédé de signature électronique, seul système susceptible d'identifier sans risque d'erreur le (ou les) signataire (s) et de manifester son (ou leur) adhésion au contenu de la déclaration ;

Considérant toutefois et en second lieu, qu'il est possible, s'agissant du dispositif mis en place cette année, de formuler un certain nombre d'observations accompagnées de recommandations propres assurer un meilleur agencement du service rendu aux contribuables ;

Considérant que le projet transmis à la CNIL prévoit que le contribuable souhaitant recourir à la téléprocédure s'identifie auprès du serveur du ministère en inscrivant « au caractère près » certains des renseignements portés sur la déclaration de revenus papier : ses nom et prénom — ou, en cas de personnes mariées, ceux de l'époux — et le numéro d'identification du foyer fiscal (numéro FIP) ; que ces éléments d'identification sont contrôlés à partir d'une base nationale de référence qui est créée pour la durée de la campagne de déclaration à partir des fichiers départementaux « FIP » et qui recense la totalité des contribuables ayant rempli une déclaration de revenus l'année précédente ; qu'à cette fin, le Ministère a également saisi la CNIL d'un projet d'arrêté modificatif concernant le traitement « FIP » de la DGI ;

Considérant que l'identification du déclarant au moyen de son numéro FIP et la transmission des fichiers de télédéclaration valent acceptation du contrat d'adhésion à la procédure de télédéclaration ; qu'inversement, le dépôt d'une déclaration papier vaut résiliation du contrat ;

Considérant qu'il ne peut être procédé qu'à un seul transfert par voie électronique par foyer fiscal ; qu'à cette fin, la base nationale de référence précitée conserve une trace de chaque déclaration reçue, identifiée par le numéro FIP du foyer fiscal, afin d'éviter les dépôts multiples ; qu'en conséquence, toute modification ultérieure d'une déclaration transmise par voie électronique doit être effectuée par courrier postal adressé au centre des impôts de rattachement du contribuable ; qu'en outre, la procédure de télédéclaration ne peut pas être utilisée par les primo-déclarants et qu'elle ne doit pas l'être par les contribuables ayant connu, au cours de l'année concernée par la déclaration, un changement dans leur état civil ou dans leur situation familiale ;

Considérant que le numéro FIP permet d'attribuer une déclaration à un foyer fiscal ; qu'en revanche, il ne permet aucune identification du ou des auteurs de la déclaration ; qu'a *fortiori,* le dispositif de l'article 170-1 bis du code général des impôts selon lequel, lorsque le foyer comprend plusieurs membres, les époux doivent conjointement signer la déclaration d'ensemble des revenus de leur foyer, perd en l'état tout caractère opératoire dans le cadre de la télédéclaration, l'engagement des deux époux, même s'il est toujours requis, ne pouvant pas être contrôlé ; qu'en conséquence, s'il est impossible de trouver, dès cette année, une solution à cette difficulté, il conviendra de la résoudre au plus tard l'an prochain ;

Considérant, en outre, que la confidentialité du numéro FIP ne peut pas être garantie dans la mesure où cet identifiant figure tant sur les formulaires papier pré-identifiés de la déclaration de revenus que sur les avis d'imposition à l'impôt sur le revenu, à la CSG et à la taxe d'habitation — du moins pour la

taxe due au titre de la résidence principale —, qui sont susceptibles d'être demandés par des personnes ou organismes souhaitant s'assurer de l'adresse ou du niveau global des revenus du contribuable ;

Considérant cependant que, moyennant un renforcement de l'information des contribuables, les règles prévues par le Ministère en ce qui concerne l'envoi d'une seule déclaration électronique par foyer fiscal et la primauté donnée en toutes circonstances aux déclarations transmises sur support papier devraient constituer une garantie suffisante contre tout établissement par l'administration de l'assiette de l'impôt du par un foyer fiscal sur la base d'une déclaration qui lui aurait été transmise à l'insu des personnes concernées ;

Considérant que si la DGI prévoit, à l'issue de la transmission des fichiers, de faire parvenir au contribuable, immédiatement un accusé de réception électronique indiquant que le transfert des déclarations énumérées sur le document informatique s'est bien ou mal déroulé sur le plan technique, et ultérieurement, par voie postale et dans les meilleurs délais, à l'adresse mentionnée sur la télédéclaration, un accusé de réception récapitulant l'ensemble des informations qu'elle comportait, un tel dispositif ne permet pas d'écarter tous risques ; que, par suite et dans l'attente d'une amélioration du dispositif d'authentification du déclarant et du contenu de la déclaration système, il conviendrait que la DGI donne instruction à ses services d'examiner avec une bienveillance toute particulière les réclamations liées à des difficultés rencontrées lors de l'utilisation de la télédéclaration ;

Considérant que l'information communiquée aux contribuables souhaitant recourir à la télédéclaration doit être de nature à pallier les lacunes du système mis en place ; qu'à cette fin, le programme de saisie des déclarations électroniques doit clairement informer les contribuables :
sur la nécessité, compte tenu des risques de saturation du réseau, de pro céder en temps utile à la télédéclaration,
sur le court délai dans lequel l'administration s'engage à lui adresser un récépissé par courrier, afin qu'il puisse, en cas de doute, faire parvenir à l'administration une déclaration « papier »,
sur la possibilité pour lui d'envoyer, jusqu'à l'expiration du délai de dé pôt de la déclaration, une déclaration papier afin de remplacer le document électronique qu'il vient de transmettre,
sur l'intérêt qu'il a à éditer les déclarations qu'il vient de transmettre à la DGI afin d'en conserver une trace,
sur l'opportunité de procéder à un effacement des fichiers transmis à la DGI de la mémoire de l'ordinateur utilisé pour l'opération lorsque le décla rant n'en est pas l'unique utilisateur ;

Considérant, en outre, qu'en cas de tentative d'envoi d'une déclaration par voie électronique au nom d'un contribuable pour le compte duquel le système de télédéclaration a déjà été utilisé, il conviendrait que le message de rejet informe l'usager des raisons du blocage et des conséquences qu'il doit en tirer ; qu'à cette fin, il pourrait être indiqué au contribuable qu'une déclaration électronique concernant son foyer fiscal a déjà été adressée à l'administration et a fait ou fera l'objet d'un récépissé qu'il devrait normalement recevoir dans les prochains jours, qu'il doit dorénavant utiliser le formulaire papier à adresser à son centre d'impôts s'il souhaite faire une nouvelle déclaration et que cette nouvelle déclaration annulera la déclaration électronique qui a été faite à son nom par le réseau Internet ;

Considérant, enfin, que l'administration devrait adresser au contribuable concerné, par envoi recommandé avec accusé de réception, non seulement les courriers qui vaudront confirmation des renseignements portés sur les déclarations effectuées par voie électronique, mais aussi, en cas de réception, pour un même foyer fiscal, de plusieurs déclarations réalisées sur support informatique ou papier, d'un courrier l'informant que seuls seront pris en compte les éléments déclaratifs portés sur le formulaire papier ;

Considérant, s'agissant des mesures de sécurité mises en place, que la protection du serveur du ministère des Finances repose sur la définition de zones d'accès logiques dont l'accès est régulé par des pare-feu ; que la zone comportant la base de données nationale de référence qui recense l'ensemble des contribuables connus est placée sur un serveur dédié et bénéficie d'un dispositif de sécurité renforcé ; qu'en outre, la DGI a pris l'engagement formel que cette base nationale sera détruite un mois après l'expiration du délai de dépôt des déclarations d'impôt sur le revenu ;

Considérant, par ailleurs, que l'ensemble des équipements du site informatique central est installé sur un plateau technique commun, dans des locaux dont l'accès est réservé aux personnels habilités et contrôlé par des lecteurs de cartes à puce ; que l'accès à chaque serveur et aux projets des différents serveurs est également réservé à des personnes spécialement habilitées ; qu'ainsi seules deux personnes pourront accéder logiquement à la base de données des contribuables et à ses sauvegardes, qui sont conservées dans la même enceinte sécurisée ;

Considérant que la DGI a également pris l'engagement que le transfert électronique des déclarations s'effectue en mode sécurisé (SSL) au moyen d'un dispositif de cryptage connu uniquement de la DGI ; que les données reçues par l'administration sont décryptées pour être intégrées dans les traitements de taxation à l'impôt sur le revenu et, dans les cas les plus complexes, pour faire l'objet d'éditions papier à destination des services compétents ; que ces opérations sont déclarées à la Commission dans le cadre d'une demande d'avis modificative relative au traitement « IR » de la direction générale des Impôts, dont l'objet est de gérer la situation des foyers fiscaux vis-à-vis de l'impôt sur le revenu ;

Considérant, enfin, que la DGI a indiqué que les transmissions de données effectuées entre le serveur et ses centres informatiques utilisent le réseau interne du Ministère et sont également chiffrées ;

Considérant que le niveau de chiffrement assuré cette année, qui est de 40 bits seulement, peut être accepté mais que la Commission a pris bonne note que la DGI a conscience de l'insuffisance de cette solution et envisage de rehausser prochainement ce niveau de chiffrement ;

Considérant que les fichiers transmis par voie électronique sont conservés dans les centres informatiques de la DGI pendant le délai de recevabilité des réclamations des contribuables tel que fixé au point a de l'article R* 196-1 du livre des procédures fiscales, c'est-à-dire pendant les deux années suivant l'année de mise en recouvrement ; que, pendant ce délai, le contribuable qui n'aurait pas reçu d'accusé de réception devrait être en mesure de demander de recevoir ce document ;

Considérant, enfin, que la DGI prévoit de retirer le système de télédéclaration du réseau Internet le lendemain de la date limite de dépôt des déclarations à 8h00 ; que cependant, une telle mesure ne tiendrait pas pleinement

compte de la dimension mondiale du réseau Internet ; qu'en effet, dès lors que le projet d'arrêté ne prévoit pas de déroger aux règles de l'article 175 du code général des impôts concernant le délai fixé pour le dépôt des déclarations, il convient que l'envoi d'une déclaration par Internet reste possible tant que la date limite fixée par l'article 175 n'aura pas été dépassée pour l'ensemble des fuseaux horaires ;

Émet, compte tenu de tout ce qui précède, **un avis favorable pour un an,** c'est-à-dire pour la durée de la campagne 2000 de l'impôt sur le revenu, sur le projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie relatif à la télédéclaration IR ainsi que sur les projets d'arrêtés modificatifs concernant les traitements « FIP » et « IR » et, dans ces conditions, sous réserve que l'article 1er du projet d'arrêté relatif à la télédéclaration IR précise que le traitement « est autorisé pour la durée de la campagne 2000 de l'impôt sur le revenu »,

Demande que soient d'ores et déjà dûment prises en compte par l'administration les recommandations précisées ci-dessus concernant :

— l'information mise à la disposition des contribuables et tout particulièrement l'envoi d'un courrier avec accusé de réception, en cas de réception, pour un même foyer fiscal, de plusieurs déclarations réalisées sur support informatique ou papier,

— la transmission aux services fiscaux d'instructions leur demandant d'examiner avec une bienveillance toute particulière les réclamations qui seraient liées à des difficultés avérées rencontrées lors de l'utilisation de la procédure de télédéclaration,

— l'information des contribuables sur le fait qu'ils peuvent demander de recevoir copie du contenu des fichiers de déclaration les concernant qui auront été transmis par voie électronique pendant les deux années suivant l'année de mise en recouvrement,

— le retrait du réseau Internet du dispositif de télédéclaration après que la date limite fixée pour le dépôt des déclarations aura été dépassée pour l'ensemble des fuseaux horaires,

Demande, en outre, dans la perspective de la mise en place du dispositif à établir pour l'année prochaine, qu'un bilan sur les conditions de mise en œuvre en 2000 de la télédéclaration soit remis à la Commission et que l'administration étudie, pour 2001, le renforcement des dispositifs de sécurité et de chiffrement, incluant la mise en place d'un procédé de signature électronique.

Délibération n° 00-013 du 22 février 2000 portant adoption du formulaire de déclaration des traitements de données personnelles mis en œuvre dans le cadre d'un site Internet.

La Commission nationale de l'informatique et des libertés,

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

Vu la directive 95/46 du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traite-

ment des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et tout particulièrement les articles 15, 16, 19 et 20, ensemble le décret n° 78-774 du 17 juillet 1978 modifié, pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu l'article 23 de la délibération n° 87-25 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 98-075 du 7 juillet 1998 portant adoption à titre expérimental d'un formulaire de déclaration des traitements automatisés d'informations nominatives mis en œuvre dans le cadre d'un site Internet et la délibération n° 99-004 du 18 février 1999 portant prorogation de l'expérimentation relative à ce formulaire ;

Vu la délibération n° 99-041 du 8 juillet 1999 portant adoption du formulaire de déclaration de déclaration des traitements de données personnelles mis en œuvre dans le cadre d'un site Internet ;

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

Considérant que, dans le souci de faciliter l'accomplissement des formalités préalables à la mise en œuvre des traitements automatisés d'informations nominatives susceptibles d'être opérés dans le cadre d'un site web, la CNIL a adopté à titre expérimental le 7 juillet 1998 (avis n° 98-075) un modèle de formulaire spécifiquement conçu pour la déclaration de tels traitements ;

Considérant que l'expérimentation de ce formulaire a été prorogée jusqu'au 1er juillet 1999 par délibération n °99-004 du 18 février 1999, puis par délibération n° 99-041 du 8 juillet 1999 pour une nouvelle période de six mois, de sorte qu'il puisse faire l'objet, le cas échéant, de toutes les adaptations qui s'avéreraient nécessaires ou contribueraient à en améliorer la lisibilité ou la rédaction ;

Considérant qu'à l'issue de ces périodes d'expérimentation, il y a lieu d'adopter de manière définitive le formulaire de déclaration dans sa présentation du 8 juillet 1999 ;

Décide d'adopter le modèle de formulaire joint en annexe.

Délibération n° 00-021 du 30 mars 2000 concernant la mise en œuvre par la direction générale de la Comptabilité publique du traitement « GIR » ayant pour objet la gestion du compte unique du contribuable en matière d'impôts directs.

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 concernant la création d'un traitement automatisé d'informations nominatives dénommé « Gestion des informations de recouvrement » (GIR),

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 l'arrêté du 28 juillet 1998 relatif à un traitement automatisé concernant le recouvrement amiable de l'impôt direct,

Vu l'arrêté du 21 août 1995 portant modification d'un traitement informatisé pour la gestion du recouvrement contentieux de l'impôt direct (RAR : restes à recouvrer),

Après avoir entendu Monsieur Noël Chahid-Nouraï en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations,

Formule les observations suivantes :

Le traitement de la direction générale de la Comptabilité publique (DGCP) dénommé « GIR » a pour objet de *créer, pour* tout contribuable, un compte fiscal unique regroupant les principales informations concernant les impôts directs émis par voie de rôle auxquels il est assujetti, quels que soient le statut de l'intéressé, la nature de l'impôt, le lieu de* taxation ou les modalités de recouvrement des sommes dues.

L'examen par la Commission de la demande d'avis relative au traitement « GIR » a plus particulièrement porté sur les finalités poursuivies, les catégories d'informations enregistrées, l'utilisation de la base par les agents de la DGCP et par les contribuables, le dispositif de sécurité envisagé et les modalités d'exercice des droits d'accès et de rectification.

Sur les finalités du traitement

La première finalité de la base nationale « GIR » est d'améliorer la diffusion de l'information sur les redevables des impôts directs auprès des agents de la DGCP chargés des opérations de recouvrement fiscal, d'une part, en organisant la circulation de l'information entre les départements informatiques du Trésor (DIT), notamment pour assurer une meilleure gestion des acomptes versés par les contribuables ayant par la suite déménagé, d'autre part, en mettant à la disposition des personnels habilités de la DGCP le compte unique des contribuables qu'ils ont à connaître, via le réseau Intranet de cette administration.

Alors que les agents chargés du recouvrement d'un impôt ne disposent actuellement que des informations se rapportant aux procédures qui relèvent de leur compétence, la consultation du compte fiscal unique devrait leur apporter une vision globale de la situation fiscale et financière des personnes, notamment des redevables défaillants (autres impôts dus ou déjà acquittés, délais accordés par d'autres services, actions en cours, situation de surendettement déjà constatée...). La mise en place de « GIR » devrait également

avoir pour effet de réduire le nombre des incidents qui surviennent lors des opérations de recouvrement forcé, à la suite d'erreurs d'homonymie.

La seconde finalité du traitement « GIR » est de rapprocher la DGCP de ses usagers, d'une part en leur proposant d'accéder directement, via Internet, le minitel ou le téléphone, à certaines informations les concernant — ou relatives à la situation fiscale des personnes morales qu'ils représentent —, d'autre part en développant et simplifiant les transactions informatiques qui sont déjà mises à leur disposition pour notifier les demandes d'adhésion à l'un des nouveaux procédés de paiement de l'impôt, pour mettre en œuvre les procédures de télérèglement de leur choix, ou pour modifier certaines informations relatives à leur situation personnelle. Une application spécifique, dénommée « SATELIT », qui reprendra la plupart des informations enregistrées dans « GIR », sera à cette fin reliée à un serveur web et à un serveur minitel.

Les deux finalités du traitement « GIR » qui viennent d'être rappelées n'appellent, à ce stade, aucune observation particulière.

Sur les catégories d'informations traitées

La plupart des informations de la base « GIR » proviendront des applications de gestion du recouvrement de l'impôt qui sont gérées dans les DIT : d'une part « REC », qui est utilisé pour la gestion de la phase amiable du recouvrement, d'autre part « RAR », qui assure la gestion de la phase contentieuse. Pour préserver la cohérence du système d'informations, la base « GIR » ne sera mise à jour qu'en aval des applications de gestion : les informations seront dans un premier temps introduites et validées dans les traitements locaux de recouvrement avant d'être communiquées par réseau à la base nationale.

Il est toutefois prévu que la base « GIR » comporte, à titre temporaire, des informations non encore validées. Cette situation concerne principalement les renseignements saisis directement par le contribuable et les données destinées à être prises en compte par plusieurs DIT. Les modalités d'affichage des informations en cours d'intégration mettront en évidence cette spécificité.

La Commission observe, dès l'abord, que la mise en place du compte unique du contribuable est rendue possible par le processus, engagé par la direction générale des Impôts, de fiabilisation et de généralisation dans les fichiers fiscaux, d'un identifiant fiscal unique, national et permanent, des personnes physiques, le numéro SPI. Elle constate avec intérêt que l'utilisation du NIR dans le cadre de la base « GIR » a pu, de ce fait, être abandonnée par l'administration, dès lors que, techniquement, le recours à cet identifiant n'est pas indispensable.

Les autres catégories d'informations traitées concernent :

— l'identité des contribuables, notamment des personnes exonérées : nom patronymique et prénoms ou raison sociale, sexe, date et lieu de naissance, adresse principale, situation familiale au regard de la législation fiscale, nombre de personnes à charge, n° SIRET, identifiants fiscaux sectoriels,

— les impositions : nature de l'impôt (impôt sur le revenu, CSG, CRDS, taxe d'habitation, taxe professionnelle, taxes foncières, taxe sur les locaux va cants, taxe de balayage, impôt sur les sociétés, imposition forfaitaire an nuelle), année d'imposition, centre des impôts et poste comptable de rattachement, numéro de rôle, montant de l'impôt, n° SPI, nom, prénoms et

adresse des codébiteurs, date de mise en recouvrement, date limite de paiement, adresse du lieu d'imposition, mode de règlement choisi pour chaque impôt (mensualisation, prélèvement à la date limite de paiement, inscription au télérèglement, télévirement référencé), références du compte bancaire ou postal de prélèvement, base annuelle de calcul du prélèvement, numéro d'enregistrement des modifications de contrat et des certificats de prise en compte de l'ordre de paiement, montant total des versements effectués, solde dû, détail du dernier versement, montant de la majoration, des pénalités de retard et des frais de poursuites,

— les informations liées à l'ouverture d'une procédure contentieuse : date de basculement dans la phase contentieuse, code « délais accordés », mon tant publié du privilège et de la créance admise en non-valeur, n° SPI, nom, prénoms ou raison sociale et adresse des tiers solidaires et des tiers déten teurs de fonds appartenant ou destinés au redevable, références des comp tes bancaires ou postaux susceptibles d'être utilisés pour le recouvrement contentieux, situation de surendettement du redevable, nature, date d'ouver ture, de publication et clôture de la procédure collective.

La base « GIR » fera l'objet d'une mise à jour quasi quotidienne. Les impositions soldées seront conservées jusqu'à l'émission des rôles de l'année suivante ou, en cas d'ouverture d'une procédure de recouvrement contentieux, au maximum pendant un an après leur solde ou la prescription de l'action en recouvrement ou, pour les créances admises en non-valeur, pendant quatre ans après leur admission.

La Commission observe que l'article 2 du projet d'arrêté n'est pas assez explicite sur les points qui viennent d'être rappelés et elle demande, en conséquence, que cette disposition soit modifiée afin, d'une part de reprendre la liste des catégories d'informations traitées telle que rappelée ci-dessus, en particulier en ce qui concerne les informations relatives à la situation financière du contribuable, d'autre part de préciser les différentes durées de conservation qui leur seront applicables.

Sur la consultation de la base « GIR » par les agents de la DGCP

Les personnels de la DGCP destinataires des informations seront :

— au sein de l'administration centrale : les agents du service chargé du trai tement des réclamations, pour l'ensemble des comptes,

— les agents des services liaison-recouvrement constitués auprès de chacun des DIT et chargés de la gestion des problèmes liés au déménagement ou au changement de nom des contribuables, pour les seuls comptes uniques des contribuables comportant au moins une imposition prise en charge dans l'un des postes de leur région informatique,

— dans les trésoreries générales, les agents du service recouvrement des im pôts, compétents pour prendre certains types de décisions (ex. : octroi d'un délai de paiement) en fonction de critères préétablis (ex. : durée du délai, montant concerné), pour les seuls comptes des contribuables dont une impo sition au moins est prise en charge dans l'un des postes comptables du dé partement,

— les personnels des recettes des finances chargés du recouvrement des im pôts, qui ont une fonction équivalente à celle des agents susmentionnés des trésoreries générales sur la base de seuils d'intervention inférieurs, pour les seuls comptes des contribuables dont une imposition au moins dépend de l'un des postes de l'arrondissement financier,

— les agents remplissant la même fonction dans les trésoreries, pour les seuls comptes des contribuables ayant au moins une imposition gérée dans le poste comptable,
— les huissiers du Trésor, pour l'exercice de leurs missions.

Il est envisagé que chaque transaction de consultation fasse l'objet d'une trace conservée pendant un mois, qui pourra être exploitée en cas de plainte pour utilisation des informations à des fins étrangères aux finalités déclarées ou sous forme de sondages ou de tableaux statistiques. Ces traces permettront d'identifier le poste utilisé, l'agent utilisateur et les comptes consultés.

La Commission considère, cependant, que la conservation pendant un mois de l'ensemble des traces de consultation n'est pas de nature à permettre un contrôle réel, notamment en cas de plainte, de l'utilisation des informations. Les risques d'exploitation à des fins personnelles par un agent des informations contenues dans la base « GIR » étant d'autant plus sérieux que son profil d'utilisateur lui permettra d'accéder à un volume plus important d'informations, la Commission demande que la durée de conservation des traces relatives aux opérations effectuées par les agents ne relevant pas d'une trésorerie locale soit notablement allongée et, plus précisément, qu'elle soit fixée à un an.

Sur l'utilisation de l'application par les contribuables

L'application « SATELIT », qui sera l'interface usagers de « GIR », proposera, à terme, aux particuliers :
— la consultation en ligne, rapide, fiable et sécurisée de la plupart des in formations connues de la DGCP sur leur situation fiscale personnelle,
— une meilleure prise en compte des opérations et événements susceptibles d'affecter leur situation au regard du paiement de l'impôt, tels que leur chan gement d'adresse,
— une extension des prestations, pour certaines déjà mises à la disposition des redevables, en relation avec les moyens modernes de règlement de l'im pôt (mensualisation, prélèvement à la date limite de paiement, adhésion au système de télérèglement, télérèglement ouvert sans adhésion préalable, té lévirement référencé),
— une simplification de l'ensemble de ces opérations, puisque l'usager dis posera, pour les effectuer, d'un identifiant unique, le numéro SPI, et éventuel lement d'un mot de passe associé.

« SATELIT » sera accessible par trois vecteurs : le téléphone, le minitel et Internet. Minitel et Internet présenteront les mêmes fonctionnalités. Celles du téléphone seront, dans un premier temps, limitées au seul paiement par télé-règlement.

La DGCP a prévu de proposer au public trois profils utilisateurs :

* Le profil n° 1 correspond au cas d'un contribuable qui souhaite consulter « SATELIT » sans utiliser son numéro SPI. Il pourra accéder à une présenta tion du logiciel. Aucun traitement de données nominatives ne sera possible dans ce cadre.

* Le profil n° 3 concerne les contribuables qui auront adhéré au service et qui, de ce fait, auront reçu un mot de passe par courrier postal. Les abonnés devront s'identifier par la double saisie de leur numéro SPI et de leur mot de passe.

Il leur sera, en premier lieu, proposé d'utiliser la procédure de télérèglement pour l'impôt de leur choix, que ce soit sur la base d'une adhésion préalable au service ou sans adhésion préalable, à condition de pouvoir s'identifier à partir des références d'un titre interbancaire de paiement pré-rempli pour régler cet impôt. Dans les deux cas, un certificat de prise en compte de l'ordre de paiement leur sera délivré par « SATELIT », qui servira de justificatif de paiement.

Ils pourront, en deuxième lieu, prendre connaissance de la plupart des éléments constitutifs de leur compte fiscal unique. Parmi les catégories d'informations enregistrées dans la base « GIR », la DGCP prévoyait, dans sa demande initiale, de ne pas autoriser la consultation par la personne concernée des rubriques suivantes : la date de basculement dans la procédure contentieuse ; le code « délais accordés » ; le montant publié du privilège ; le montant de l'admission en non-valeur ; les numéros SPI, nom, prénoms et adresse des codébiteurs de l'impôt ; les numéros SPI, nom, prénoms et adresse des tiers solidaires ; les identifiant, nom, prénoms ou raison sociale et adresse des tiers détenteurs de fonds ; les coordonnées bancaires utilisées dans le cadre d'une procédure contentieuse ; les informations relatives à la procédure collective.

La Commission considère cependant que seules les informations enregistrées dans « GIR » dont la communication risquerait de porter atteinte au bon déroulement des opérations de recouvrement forcé devraient être exclues de « SATELIT » et que cette définition ne correspond ni au nom des codébiteurs de l'impôt, ni au code « délais accordés ». Elle demande, en conséquence, que ces informations puissent être consultées via l'application « SATELIT » par les personnes concernées.

En dernier lieu, le profil utilisateur n° 3 donnera la possibilité aux adhérents de procéder aux modifications suivantes : changer l'adresse principal du contribuable, le mode de paiement, les références bancaires ou postales utilisées pour le prélèvement ou le télérèglement, la base annuelle de calcul des prélèvements en cas de mensualisation, le montant du prélèvement effectué à la date limite de paiement, refuser l'étalement du solde à payer (en cas de forte augmentation d'un impôt payé par mensualités), renoncer au prélèvement à la date limite, changer l'unité monétaire de son contrat de mensualisation ou de prélèvement à la date limite.

Chaque opération de modification se traduira par la communication par « SATELIT » d'un numéro d'enregistrement, qui sera conservé par le DIT chargé de notifier la modification au contribuable et attestera de la demande adressée en ligne par le contribuable en cas de réclamation. Un accusé de réception papier sera transmis par voie postale. Enfin, un accusé de réception électronique pourra être envoyé via Internet pour les contribuables ayant laissé leur adresse e-mail. Cette information ne sera conservée par la DGCP que le temps de l'envoi de l'AR et l'article 2 du projet d'arrêté devra être complété sur ce point.

* Le profil n° 2 concernera les contribuables qui sont disposés à s'identifier à partir du numéro SPI mais n'ont pas demandé à bénéficier d'un mot de passe. Il ne pourra être utilisé que par minitel ou Internet. Ces usagers devraient avoir la possibilité de procéder à l'ensemble des modifications autorisées par « SATELIT ». Ils devront, cependant, réaliser ces opérations « en aveugle », c'est-à-dire qu'ils ne pourront pas consulter les informations portées dans leur compte fiscal unique. Le dispositif de confirmation des transac-

tions effectuées décrit ci-dessus au sujet du profil n° 3 sera repris dans le cadre du profil d'utilisateur n° 2.

La Commission comprend le souci de la DGCP de ne pas gêner le développement des services sur Internet en imposant aux usagers potentiels des contraintes trop lourdes qui ne pourraient que les décourager d'utiliser le nouveau service. Elle tient notamment compte du fait qu'un accusé de réception papier sera systématiquement transmis par voie postale pour toute opération, ce qui devrait donner à l'intéressé la possibilité de réagir avant que soit prise en compte une demande qui ne serait pas conforme à sa volonté.

La Commission estime, cependant, que la mise en place sur minitel ou Internet d'un service permettant la modification de données nominatives, dont l'ouverture n'est pas conditionnée à l'adhésion préalable des personnes concernées et dont les procédures d'accès ne sont pas sécurisées par l'emploi d'un mot de passe, ne peut être envisagée qu'à la condition qu'un droit d'opposition soit reconnu aux intéressés. En conséquence, la Commission demande que les personnes ne souhaitant pas que les informations les concernant soient consultables via le serveur « SATELIT » puissent s'y opposer et que le public soit clairement informé de ce droit.

Sur le dispositif de sécurité envisagé par la DGCP

La Commission prend acte de ce que :
— le niveau de sécurité constituera l'un des principaux critères pris en compte dans l'appel d'offre pour la désignation du prestataire informatique chargé de la mise en œuvre de la base « GIR »,
— l'application fonctionnera dans un environnement qui lui sera exclusive ment dédié et dont les accès auront été sécurisés, sur des machines et dispo sitifs techniques également dédiés et avec un personnel spécifiquement affecté à « GIR »,
— il est exclu que les fichiers « GIR » puissent faire l'objet d'une procédure de téléchargement,
les sauvegardes seront cryptées,
— il n'y aura aucun accès direct à « GIR » par le web,
— des pare-feu associés à un système de surveillance des lignes garantiront contre toute intrusion dans le fichier,
— aucun des postes de travail des agents de la DGCP ne servira à la fois à la consultation d'Internet et de l'Intranet de la DGCP, utilisé notamment pour la consultation de « GIR ».

La Commission constate, toutefois, que les mesures de sécurité effectivement mises en place dépendront, pour une large part, des résultats de l'appel d'offres lancé à cette fin. Elle demande, en conséquence, que lui soit communiqué un descriptif de l'architecture technique de la base qui sera retenue ainsi que des mesures de sécurité envisagées, lorsque ces éléments auront été arrêtés en concertation avec le prestataire informatique chargé de la mise en œuvre du

La Commission considère, par ailleurs, qu'il convient de reconnaître au fichier « GIR » un caractère particulièrement sensible, qui tient au fait qu'il recensera une proportion très large de la population, que les éléments d'identité y figurant auront normalement été *certifiés par l'INSEE, que la*

mise à jour des adresses enregistrées dans la base bénéficiera des prérogatives reconnues par la loi à l'administration fiscale et que la consultation de « GIR » permettra, à terme, de déduire certaines informations protégées par l'article 31 de la loi du 6 janvier 1978.

En conséquence de ce qui précède, la Commission estime qu'il y a lieu pour la DGCP, d'une part, de prendre en compte ces risques, d'autre part, de prévoir, conformément à l'article 21-3° de la loi du 6 janvier 1978, un dispositif garantissant la prise, en cas de circonstances exceptionnelles, de mesures de sécurité appropriées pouvant aller jusqu'à la destruction des supports d'information de la base.

Sur l'exercice des droits d'accès et de rectification

Les modalités pratiques d'exercice de ces droits seront données en ligne aux usagers et dépendront du type d'information concernée :

— Lorsqu'il s'agira d'une demande de rectification correspondant à l'un des cas envisagés dans « SATELIT », celle-ci sera automatiquement adressée au service local compétent. Un numéro d'enregistrement sera communiqué au contribuable et il appartiendra au service compétent de l'informer de la rectification en mentionnant ce même numéro.

— Lorsque la demande visera à obtenir la modification d'autres informa tions ou à accéder à des informations conservées par le Trésor public qui ne figurent pas dans le compte unique, l'usager pourra prendre connaissance des références du service auprès duquel il doit accomplir sa démarche. *Sur ce dernier point, il serait souhaitable que les démarches à accomplir en cas de contestation de l'assiette de l'un ou l'autre des impôts inscrits dans le compte fiscal unique soient également décrites.*

Compte tenu de ces observations, la Commission :

Émet un avis favorable sur le projet d'arrêté qui lui est soumis par le ministère de l'Economie, des Finances et de l'Industrie, **sous réserve :**

— que l'article 2 du projet d'arrêté soit modifié conformément à ce qui a été dit ci-dessus afin, d'une part de reprendre la liste des catégories d'informa tions traitées, en particulier en ce qui concerne les informations portant sur la situation financière et l'adresse e-mail du contribuable, d'autre part de préci ser les différentes durées de conservation qui leur sont applicables ;

— que la durée de conservation des traces relatives aux opérations effec tuées par les agents de la DGCP ne relevant pas d'une trésorerie locale soit fixée à un an ;

— que l'identité des codébiteurs et le code « délais accordés » soient ajou tés à la liste des informations de « GIR » susceptibles d'être consultées via le minitel ou Internet par le contribuable concerné ;

— qu'un droit d'opposition soit reconnu aux contribuables qui ne souhaite raient pas bénéficier des services de « SATELIT », que ceux-ci en soient clai rement informés et que l'article 6 du projet d'arrêté soit modifié en ce sens ;

— que soit communiqué à la Commission un descriptif de l'architecture tech nique de la base qui sera retenue ainsi que des mesures de sécurité envisa gées lorsque ces éléments auront été fixés en concertation avec le prestataire informatique chargé de la mise en place du traitement « GIR », ces mesures devant prendre en compte d'une part les risques accrus d'atteinte à la sécuri té (interception notamment) liés au développement des réseaux, d'autre part

les nouveaux procédés techniques et juridiques d'authentification des usagers ;
— que, conformément à l'article 21-3° de la loi du 6 janvier 1978, la DGCP prévoie qu'en cas de circonstances exceptionnelles, un dispositif de sécurité approprié soit mis en place, pouvant aller jusqu'à la destruction des informations du Répertoire et dont le détail devra être soumis à la CNIL.

Délibération n° 00-022 du 30 mars 2000 portant avis sur un projet de décret présenté par le ministère de l'Agriculture relatif à la communication d'informations par les caisses de la mutualité sociale agricole aux commissions chargées d'établir les listes électorales pour les élections aux chambres d'agriculture.

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, notamment son article 5 ;

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

Vu le code rural ;

Vu le code de la sécurité sociale ;

Vu la loi n° 95-95 du 1er février 1995 de modernisation de l'agriculture ;

Vu le projet de décret présenté par le ministère de l'Agriculture ;

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

Considérant que la Commission nationale de l'informatique et des libertés est saisie par le ministère de l'Agriculture d'un projet de décret visant à organiser la transmission, par les caisses départementales et pluridépartementales de mutualité sociale agricole et les caisses générales de sécurité sociale dans les départements d'Outre-mer, d'informations nominatives concernant les électeurs aux commissions départementales chargées de l'établissement des élections des membres des chambres d'agriculture ;

Considérant que l'article 77-1 de la loi n° 95-95 du 1er février 1995 dispose que « pour l'établissement des listes électorales aux élections aux chambres d'agriculture, qui auront lieu au-delà du 31 janvier 1995, les commissions communales et départementales peuvent obtenir les renseignements nécessaires détenus par les caisses départementales et pluridépartementales de mutualité sociale agricole dans les départements métropolitains, par les caisses générales de sécurité sociale, organismes gestionnaires des cotisations et de prestations de personnes concernées dans les départements d'Outre-mer. Un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent alinéa » ;

Considérant que les conditions pour être inscrit sur les listes électorales des élections aux chambres d'agriculture supposent, pour trois des quatre collèges électoraux concernés, l'affiliation à un régime de protection sociale agricole ; que les informations transmises par les caisses susvisées aux commissions départementales sont destinées à leur permettre d'effectuer un contrôle de cohérence des informations et vérifier le collège électoral d'appartenance des électeurs ;

Considérant que les informations transmises par les caisses aux commissions départementales prévues par l'article R. 511-16 du nouveau du code rural sont relatives au nom, prénoms, date et lieu de naissance, à la mention selon laquelle la personne est ressortissante de l'Union européenne, à l'adresse, à la commune du siège de l'exploitation agricole ou du lieu de travail effectif et à la catégorie au titre de laquelle l'intéressé est affilié ;

Considérant qu'il est précisé que les informations transmises seront détruites dès lors que les listes électorales seront définitives ; que cette destruction sera effectuée sous la responsabilité du Préfet qui prendra toutes mesures utiles afin de veiller à la sécurité et à la confidentialité de ces informations ;

Émet, sous réserve de l'adoption du projet de décret en Conseil d'Etat joint au présent projet de décret soumis à l'avis de la CNIL, un avis favorable au projet de décret présenté par le ministère de l'Agriculture.

Délibération n° 00-023 du 30 mars 2000 portant avis sur un projet de décret présenté par le secrétariat d'État à l'Outre-mer relatif à la création d'un traitement automatisé nécessaire à la tenue du fichier général des électeurs inscrits en Nouvelle-Calédonie.

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, notamment son article 5 ;

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

Vu la loi v99-209 du 21 mars 1999 relative à la Nouvelle-Calédonie, et notamment son titre V ;

Vu le projet de décret présenté par le secrétaire d'État à l'Outre-mer ;

Après avoir entendu Monsieur Maurice Benassayag en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que la Commission nationale de l'informatique et des libertés est saisie par le Secrétariat d'État à l'Outre-mer d'un projet de décret visant à créer un traitement informatisé constituant le fichier général des électeurs ; que la création du fichier général des électeurs inscrits sur les listes électorales de Nouvelle-Calédonie est prévue par l'article 189-VII de la loi organique n° 99-209 du 19 mars 1999 relative à la Nouvelle-Calédonie ; que le

même article confie la tenue de ce fichier à l'Institut territorial de la statistique et des études économiques de Nouvelle-Calédonie ;
Considérant que le fichier général des électeurs comprend les listes électorales de Nouvelle-Calédonie (listes générales), les listes électorales établies en vue de la consultation organisée le 8 novembre 1998 en application de l'article 76 de la Constitution et leur historique (liste spéciale), les listes électorales complémentaires pour l'élection au Parlement européen par les ressortissants de l'Union non français mais demeurant sur le territoire français et les listes électorales complémentaires pour l'élection des conseils municipaux par les ressortissants de l'Union européenne non français ; Considérant que le fichier général des électeurs est mis à jour à partir des décisions d'inscription ou de radiation des commissions administratives chargées de réviser les listes électorales, des décisions des commissions administratives spéciales chargées d'établir la liste électorale spéciale et le tableau annexe des électeurs, des demandes d'inscriptions sur la liste électorale spéciale, des décisions judiciaires relatives à l'inscription ou à la radiation d'un électeur, des avis de perte ou de recouvrement de capacité électorale transmis par le casier judiciaire, des avis de décès établis par les mairies, ainsi que des avis reçus de l'INSEE ou des représentants de l'Etat chargés, à Mayotte, en Polynésie française et dans les îles de Wallis et Futuna, du contrôle des listes électorales demandant la radiation d'un électeur des listes de Nouvelle-Calédonie, ou informant du décès d'un électeur ou encore faisant part d'une décision privative des droits civils et politiques hors de la Nouvelle-Calédonie ; Considérant que les catégories d'informations traitées sont relatives à l'identité de l'électeur, à la date et au lieu de la demande d'inscription, à la date de l'inscription, au type de liste électorale, à l'admission de l'électeur à participer à la consultation du 8 novembre 1998 et à l'historique de cette admission, à la perte des droits civils et politiques (date d'effet et durée), à l'acquisition ou à la perte de la nationalité française, au décès et à la nationalité pour les ressortissants de l'Union européenne ;
Considérant que les destinataires des informations traitées sont le Haut-Commissariat de la République en Nouvelle-Calédonie, qui informe le Gouvernement de l'évolution du corps électoral, les maires de Nouvelle-Calédonie pour les électeurs inscrits dans leur commune, l'INSEE et, à Mayotte, en Polynésie française et dans les îles de Wallis et Futuna, le représentant de l'Etat chargé du contrôle des listes électorales, ainsi que les magistrats présidant les commissions administratives spéciales de révision des listes électorales ; Considérant que le projet de décret rappelle que le fichier général des électeurs ne peut pas être utilisé à des fins de recherche des personnes ; Considérant que le droit d'accès des personnes concernées s'exercera, en application de l'article 34 de la loi du 6 janvier 1978, auprès de l'Institut Territorial de la Statistique et des Etudes économiques de Nouvelle-Calédonie ;
Émet un avis favorable au projet de décret présenté par le Secrétaire d'Etat à l'Outre Mer.

Délibération n° 00-031 du 25 mai 2000 portant avis sur le projet d'acte réglementaire présenté par le CRÉDOC et concernant la mise en œuvre d'une base de données statistiques dans le cadre de l'observatoire des entrées et sorties du dispositif RMI à Paris.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le directeur général du CRÉDOC d'un projet de décision concernant la mise en œuvre d'une base de données statistiques dans le cadre de l'observatoire des entrées et sorties du dispositif RMI à Paris,

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 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 modifié pris pour son application,

Après avoir entendu Monsieur Pierre Schapira en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations,

Formule les observations suivantes :

Sur les finalités du traitement

La Commission nationale de l'informatique et des libertés est saisie par le Centre de recherche pour l'étude et l'observation des conditions de vie (CRÉDOC) d'une demande d'avis concernant la constitution d'une base de données statistiques en vue d'évaluer les politiques d'insertion des allocataires parisiens du revenu minimum d'insertion et en particulier de mieux connaître les circonstances d'entrée et de sortie du dispositif du RMI.

Le traitement constituera le premier volet de l'observatoire des entrées et des sorties du dispositif RMI à Paris, mis en place à l'initiative de la Préfecture (DASS) et du Département de Paris (DASES) dans le cadre du programme départemental d'insertion et confié au CRÉDOC.

Sur la nature des informations traitées

La mise en œuvre de la base de données statistiques nécessitera l'appariement d'informations préalablement anonymisées issues des fichiers de l'ANPE d'Île-de-France, de la CAF de Paris, de la CNAF, du CNASEA d'Ile-de-France, de la cellule centrale de coordination de la DASES et de l'URSSAF de Paris, organismes partenaires de l'observatoire. Ces variables seront issues des dossiers de demande de RMI détenus par la CAF de Paris dans le cadre de sa mission d'organisme payeur, des contrats d'insertion traités par la cellule centrale de coordination de la DASES, des déclarations uniques d'embauche envoyées à l'URSSAF, des dossiers de stages rémunérés et de contrats emploi solidarité ou consolidé gérés par le CNASEA, des

demandes d'emploi traitées par l'ANPE, ainsi que du fichier national de contrôle du RMI mis en place par la CNAF.

La Commission relève que doit figurer au titre des variables utilisées dans la base de données statistiques la nationalité des personnes concernées sous la forme : « Français, ressortissant Union européenne, étranger hors Union européenne ». Le CRÉDOC fait valoir que cette information, sous cette forme, serait de nature à appréhender les difficultés à maîtriser la langue française, élément pouvant constituer un frein à l'insertion.

La Commission estime toutefois nécessaire de disposer, à l'issue de la réalisation du premier volet de l'observatoire, d'une évaluation de la pertinence des variables utilisées, et en particulier de celles relatives à la nationalité.

Sur les mesures de sécurité envisagées

Une convention avec l'ensemble des partenaires de l'observatoire précisera les modalités de mise en œuvre de la base de données statistiques et comportera, en particulier, un engagement du CRÉDOC à ne pas traiter les informations détenues dans le cadre de l'observatoire à d'autres fins que celles exprimées au sein de la demande d'avis présentée à la CNIL.

Les données issues des organismes partenaires de l'observatoire seront anonymisées préalablement à leur transmission au CRÉDOC.

Cette anonymisation sera réalisée au moyen d'un algorithme de hachage irréversible intégré au logiciel FOIN (fonction d'occultation des informations nominatives) mis en place par le Centre d'études des sécurités du système d'information de la CNAMTS et validé par le SCSSI. Cet algorithme produira, soit à partir du matricule CAF et du sexe des allocataires, soit à partir de leur numéro de sécurité sociale (NIR), des « numéros d'anonymat » qui permettront d'agréger les informations relatives à une même personne sans que l'identité de cette personne puisse être connue du responsable du traitement statistique. En outre, aussitôt l'appariement des données effectué par le CRÉDOC, les numéros produits par l'algorithme seront détruits. Ainsi, à l'expiration de cette opération, la base de données statistiques sera purement anonyme et ne permettra plus, ni directement, ni indirectement, d'identifier les personnes concernées.

La Commission considère que le recours à cette fonction d'occultation des informations nominatives garantit de façon satisfaisante l'anonymat des données traitées dans le cadre de l'observatoire.

Sur l'information des personnes concernées par le traitement

Les personnes concernées seront informées de la mise en œuvre du traitement par affichage de l'acte réglementaire du CRÉDOC dans les locaux des organismes partenaires.

En outre, il convient que l'ensemble de ces organismes diffuse, par voie d'affichage ou d'insertion dans les périodiques susceptibles d'être adressés à l'ensemble des allocataires du RMI, une information claire sur la finalité et les modalités de mise en œuvre de l'observatoire.

Compte-tenu de ces observations, la Commission :
— **émet un avis favorable** au projet d'acte réglementaire présenté par le directeur général du CRÉDOC,

demande aux organismes *partenaires* de l'observatoire la diffusion, par voie d'affichage ou d'insertion dans les périodiques susceptibles d'être adressés à l'ensemble des allocataires du RMI, d'une information claire sur les modalités de mise en oeuvre de l'observatoire,

— **demande** à être saisie, à l'issue de la mise en œuvre de la première phase de l'observatoire, d'un bilan de réalisation de l'opération d'apparie ment des données et d'un bilan évaluant la pertinence de la taille des échan tillons retenus ainsi que des variables utilisées, et en particulier de celles relatives à la nationalité.

Délibération n° 00-034 du 8 juin 2000 relative à la modification des procédures de télétransmission des déclarations fiscales professionnelles.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le ministre de l'Economie, des Finances et de l'Industrie :
d'un projet de décret « pris pour l'application des articles 1649 quater B bis et 1649 ouater B quater du code général des impôts et relatif à la trans mission des déclarations fiscales professionnelles par voie électronique »,
d'un projet d'arrêté « 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 »,
d'un projet d'arrêté « relatif à la mise en service par la direction générale des Impôts d'un traitement automatisé de collecte des données fiscales et comptables » (« TDFC »),

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, ensemble le décret n° 79-1037 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques, notamment ses articles 12 et 13,

Vu la loi n° 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle, notamment ses articles 1 et 4,

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,

Vu le code général des impôts, notamment les articles 1649 quater B bis et 1649 quater B quater,

Vu le livre des procédures fiscales, notamment les articles L. 170, L. 186 et R* 196-1,

Vu le code des marchés publics, notamment les articles 48 et 52 à *55,* Après avoir entendu Monsieur Noël Chahid-Nouraï en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations,

Formule les observations suivantes :

Le traitement de la direction générale des Impôts (DGI) dénommé « transfert de données fiscales et comptables » (« TDFC »), qui fait l'objet de la saisine pour avis, permet aux entreprises commerciales, agricoles ou libérales de faire parvenir à l'administration fiscale, sur support magnétique ou via le réseau de télécommunication, leurs déclarations de résultats, les liasses fiscales ainsi que tout document qui les accompagnent. Les opérations techniques d'échange de données informatisé sont réalisées le plus souvent par un intermédiaire technique habilité par la DGI, dénommé « partenaire EDI » (échange de données informatisé), spécialement mandaté à cet effet par le contribuable. Elles peuvent également l'être par le contribuable lui-même, sous réserve qu'il ait obtenu la qualité de partenaire EDI.

Les projets soumis à la CNIL prévoient, d'une part, l'instauration d'un nouveau cadre juridique qui s'applique à l'ensemble des téléprocédures fiscales mises, à terme, à la disposition des entreprises, d'autre part, l'aménagement du seul dispositif actuellement en vigueur, la procédure « TDFC ».

/. *Sur la mise en place d'un cadre juridique général pour les déclarations dématérialisées des entreprises*

Le dispositif proposé comporte, plus précisément, un projet de décret pris pour l'application des articles 1649 quater B bis et 1649 quater B quater du CGI et un projet d'arrêté 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.

Les modalités de la transmission électronique de l'ensemble des déclarations professionnelles, qui sont identiques quels que soient l'impôt considéré et le mode de transmission électronique utilisé, sont fixées, lorsque la procédure est facultative, par un contrat d'adhésion qui lie l'administration au contribuable, et lorsqu'elle a un caractère obligatoire en application de l'article 1649 quater b quater du CGI, par arrêté du ministre chargé du budget. *La Commission prend acte de ce que, pour chaque catégorie de déclaration professionnelle, les modalités de transmission et de traitement correspondantes sont définies par arrêté du ministre compétent pris après avis de la CNIL*

Le projet de décret prévoit que chaque partenaire EDI, qu'il agisse pour son compte propre ou pour celui de ses mandants, conclut également avec l'administration fiscale, au vu d'un cahier des charges, une convention conforme au modèle défini par le projet d'arrêté susmentionné, qui formalise leurs engagements respectifs. La nouvelle convention-type sera adressée à l'ensemble des partenaires EDI recensés. Toutefois, les conventions conclues en application des dispositions antérieures seront prorogées.

Le projet de convention type — qui revêt la forme d'un arrêté — prévoit qu'un partenaire EDI n'est pas autorisé à sous-traiter l'envoi des télédéclarations fiscales à un organisme n'ayant pas obtenu lui-même la qualité de partenaire EDI. Lorsque cette condition est remplie, le partenaire initialement mandaté a pour seule obligation d'en informer sa clientèle.

Les annexes de la demande d'avis — mais non le projet de décret, ni le projet d'arrêté — prévoient que la qualité de partenaire EDI est reconnue au terme d'une procédure d'habilitation qui comporte une phase administrative, au cours de laquelle la « moralité publique » du demandeur est examinée, et une phase technique qui se limite à l'analyse de la description faite par le candidat des moyens techniques qu'il mettra en œuvre pour procéder aux transmissions. L'étude de la moralité du demandeur est effectuée sur la base des critères définis pour les personnes souhaitant être admises à concourir aux marchés de l'État (absence de faillite personnelle, régularité de la situation au regard des impôts, taxes et cotisations sociales). Les seules informations prises en compte par l'administration consistent dans les certificats, attestations ou déclarations, délivrés par les administrations et organismes compétents, que le candidat doit produire.

La *Commission observe, en ce qui concerne la phase administrative, que la procédure d'habilitation des candidats au titre de partenaire EDI, qui - sans texte spécial le prévoyant explicitement — suit les règles du code des marchés publics applicables aux personnes souhaitant soumissionner aux marchés de l'Etat alors qu'il ne s'agit pas de marchés publics, ne peut être regardée comme étant conforme aux dispositions en vigueur.*

Les autres dispositions des projets de décret et d'arrêté relatifs à la transmission par voie électronique des déclarations fiscales professionnelles n'appellent pas d'observation particulière.

II. Sur les modalités de transfert et de traitement propres à la procédure « TDFC »

En ce qui concerne la transmission des informations fiscales et comptables

Les autres documents de la demande d'avis modificative, notamment le projet d'arrêté relatif à la mise en service par la direction générale des Impôts d'un traitement automatisé de collecte des données fiscales et comptables, se rapportent exclusivement au dispositif relatif à l'envoi, sous une forme dématérialisée, des déclarations de résultats et de leurs annexes.

Les contribuables susceptibles d'adhérer à ce système sont :
— les entreprises soumises à l'impôt sur les sociétés, y compris les groupes de sociétés, ou à l'impôt sur le revenu (IR) dans la catégorie des bénéfices in dustriels et commerciaux relevant d'un régime réel d'imposition,
— les contribuables soumis à l'IR dans la catégorie des bénéfices non com merciaux relevant du régime de la déclaration contrôlée,
— les contribuables soumis à l'IR dans la catégorie des bénéfices agricoles relevant d'un régime réel d'imposition.

Deux formules d'adhésion leur sont actuellement proposées :
— *l'adhésion partielle* permet de ne transmettre que leur liasse fiscale, à l'exclusion des autres documents (déclaration de résultats, annexes signées). Elle se traduit par la simple apposition d'une mention dans une case réservée à cet effet sur la première page de la déclaration de résultats papier corres pondante. Cette adhésion doit être renouvelée chaque année ;
— *l'adhésion globale* concerne la transmission de l'ensemble des éléments déclaratifs, notamment de la plupart des annexes (relevé de frais généraux, attestation d'adhésion délivrée par l'organisme de gestion agréé, annexes libres...). Elle suppose la souscription d'un contrat d'adhésion à « TDFC »,

qui doit être déposé auprès du centre des impôts de rattachement au plus tard à la date limite du dépôt papier. Ce contrat mentionne les coordonnées du partenaire EDI qui a été choisi pour assurer la transmission des documents fiscaux.

La convention « TDFC », dont le texte est modifié par le projet d'arrêté soumis à la CNIL, est conclue pour une durée d'un an à compter de la date de la signature et renouvelable par tacite reconduction. Les contribuables peuvent, à tout moment, renoncer au bénéfice de la procédure « TDFC » en déposant une déclaration de résultats sur support papier, pour ceux qui ont opté pour la transmission globale, ou tout ou partie de la liasse sur support papier, pour ceux qui ont choisi l'adhésion partielle.

Par ailleurs, la procédure de la transmission globale sera systématiquement appliquée à partir de 2001 aux contribuables ayant, au titre de l'article 1649 quater B quater du code général des impôts, l'obligation de souscrire par voie électronique leurs déclarations d'impôt sur les sociétés. Alors que deux modes de transmission des fichiers émis par les partenaires EDI sont actuellement utilisés : depuis l'origine, le support magnétique (bande ou cartouche magnétiques) et, depuis 1992, la télétransmission, l'administration fiscale envisage, désormais, la mise en place d'une nouvelle application, dénommée « EDI-TDFC », conforme à la norme internationale EDIFACT-ONU. La dématérialisation du dépôt des documents fiscaux et comptables a été engagée par la DGI dès 1991 sur un format « propriétaire ». Or, depuis une circulaire du Premier ministre en date du 16 janvier 1997, les administrations doivent recourir, pour leurs échanges dématérialisés, à la norme EDIFACT, actuellement utilisée de façon prédominante en France et dans le monde.

« EDI-TDFC » présente l'avantage d'assurer l'identité de langage de l'émetteur déclarant au récepteur au sein de la DGI. Les opérations de conversion d'un langage à l'autre ne seront plus nécessaires au niveau du partenaire EDI ou des logiciels de comptabilité. En outre, les messages EDIFACT utilisés pour la procédure « EDI-TDFC » seront compris de la profession comptable, des banques, des tribunaux de commerce, des administrations..., permettant ainsi, à terme, à un même émetteur de transmettre simultanément les informations à plusieurs destinataires.

Le format antérieur, dit « TDFC traditionnel », sera maintenu pendant une période de transition afin de permettre aux partenaires de la DGI de modifier leurs traitements.

L'ensemble de ces modalités n'appelle pas d'observations particulières.

Depuis 1994, la procédure prévoit le recours à un dispositif de sécurisation électronique, qui est mis en place pour :

— les partenaires EDI ayant décidé de mettre en place la nouvelle procé dure « EDI-TDFC » ;

— ceux qui adhèrent à la procédure « TDFC traditionnel », mais qui ont choisi d'effectuer la transmission des déclarations de résultats et autres docu ments signés.

Par sécurisation électronique, on fait référence à un dispositif technique qui donne à un document sous forme électronique la même valeur administrative et juridique qu'un document papier signé.

Elle assure au partenaire EDI, auteur de l'échange, la garantie qu'il sera identifié de manière irréfutable par la DGI, que les données signées ne pour

ront plus être modifiées au cours ou après l'échange, que tous les éléments de sécurité sont archivés et qu'en cas de détournement du dispositif de sécurisation du partenaire EDI, le système sera immédiatement mis en opposition.

Le partenaire EDI qui désire mettre en œuvre la sécurisation des données doit disposer d'une bibliothèque de fonctions de sécurité, d'un jeu de cartes à microprocesseur contenant ses éléments d'identification — appelé « certificat » —, d'une clé publique et d'une clé secrète d'échange, et d'un lecteur de cartes à microprocesseur. Lors de son agrément, le partenaire EDI reçoit de la DGI un certificat qui l'authentifie. Au cours de l'échange, le partenaire EDI transmet son certificat, la clé d'échange publique qui permettra à la DGI de déchiffrer sa signature, et une signature de la DGI garantissant ces éléments d'identification.

Par ailleurs, la valeur juridique des documents informatiques transmis sans recours au procédé de sécurisation électronique devrait, en toute hypothèse, être reconnue dès lors que seront réunies les conditions posées par la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique :

— l'identification de la personne dont émanent les documents ;

— l'établissement et la conservation de ceux-ci dans des conditions propres à en garantir l'intégrité.

La Commission observe, en revanche, que les informations, qui sont accompagnées du résultat de la sécurisation et du certificat de l'émetteur, sont transmises en clair par le partenaire EDI à la DGI.

La DGI justifie cette solution par la décision, prise au moment de l'étude préalable de « TDFC », de placer les transmissions dématérialisées et les échanges papier sur un même niveau de confidentialité.

Elle fait également observer que les informations transmises ont un caractère public pour la plupart des entreprises concernées par « TDFC » qui ont l'obligation de publier leurs comptes. Elle ajoute que la messagerie X400 ou le protocole PESIT sur TRANSPAC offre une garantie suffisante contre les intrusions. Elle annonce, enfin, qu'une étude sera prochainement lancée en vue d'utiliser Internet comme environnement d'échange et que, dans ce cas, le message transmis pourrait être chiffré.

La Commission considère, s'agissant de l'argument relatif à la publicité légale des comptes annuels que ce dispositif ne s'applique pas à l'ensemble des sociétés commerciales et civiles (ex. : certaines sociétés en nom collectif ou en commandite simple) et qu'a fortiori, *elle ne concerne jamais les personnes physiques ayant la qualité de commerçant, artisan ou exerçant une profession libérale, qui sont cependant susceptibles d'adhérer à « TDFC ». En outre, et en toute hypothèse, l'argument ne vaut ni pour l'ensemble des annexes transmises via « TDFC », ni pour la déclaration fiscale de résultats dont le contenu est soumis au secret fiscal.*

L'exemple récent de la procédure de transmission par Internet des déclarations de revenu montre que la DGI a parfois recours à des dispositifs de cryptage pour préserver la confidentialité des informations qui lui sont transmises et il paraît difficile de justifier que les déclarations de bénéfices industriels et commerciaux, de bénéfices non commerciaux ou de bénéfices agricoles ne bénéficient pas des mêmes garanties que les déclarations d'ensemble des revenus des mêmes personnes physiques.

En conséquence, la Commission insiste sur l'intérêt qu'il y aurait pour l'administration à mettre en place, à terme, conformément aux orientations générales du ministère de l'Economie, des Finances et de l'Industrie, un dispositif technique permettant à chaque déclarant de choisir le degré de confidentialité dont il souhaite bénéficier — y compris à 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.

La Commission demande, par ailleurs, que, jusqu'à la mise en place de ce dispositif de cryptage dont elle souhaite qu'elle intervienne dans les meilleurs délais, les contribuables adhérents à « TDFC » soient clairement informés de ce que les informations les concernant sont transmises en clair 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 et de conservation des informations par les partenaires EDI

La DGI propose, afin de prévenir la conservation, par le partenaire EDI, des informations au-delà du temps nécessaire aux opérations de transmission par voie électronique, que le cahier des charges de l'application indique que toute conservation ou utilisation des données au-delà du temps nécessaire à leur transmission et à leur bonne réception par la DGI s'écarte de la procédure TDFC, et relève, s'agissant des conditions de mise en œuvre de traitements informatisés, de la loi n° 78-17 du 6 janvier 1978. Le projet d'arrêté « TDFC » indique, par ailleurs, que le partenaire EDI ne peut conserver les informations au-delà de ce qu'impose la procédure de télédéclaration qu'avec l'accord du contribuable et pour la réalisation d'opérations effectuées à sa demande.

En outre, le partenaire EDI pourra transmettre, à des organismes tiers (organismes de gestion agréés, banques, tribunaux de commerce...) et sous les formats définis pour les téléprocédures fiscales, les données informatiques relatives aux renseignements comptables et fiscaux à la condition qu'il respecte les prescriptions de la loi du 6 janvier 1978, que la transmission ait été expressément autorisée par le contribuable et que le numéro fiscal FRP ne fasse pas partie des données transmises.

Ces dernières dispositions n'appellent pas d'observations particulières.

En ce qui concerne les modalités d'exploitation et de conservation des informations par la DGI

Le centre régional informatique (CRI) de Nevers assure la réception des envois dématérialisés. Il vérifie la qualité des données avant de les communiquer aux autres CRI en fonction de leur compétence territoriale, en vue de leur utilisation. Les informations sont, en premier lieu, intégrées dans les chaînes de traitement de l'application « FNDP ». En second lieu, les déclarations professionnelles sont mises à la disposition des seuls agents des recettes et des centres des impôts chargés de l'assiette, du contrôle et du recouvrement, en fonction des règles de compétence territoriale, soit sous forme d'éditions papier, soit en consultation à l'écran.

Le projet d'arrêté « TDFC » indique que la durée de conservation des informations est définie par référence à l'article R* 196-1 du livre des procédures fiscales (LPF) qui définit, sauf dérogations particulières, le délai général de

réclamation en matière fiscale : deux ans après l'année, suivant le cas, de la mise en recouvrement du rôle ou le versement spontané de l'impôt. Toutefois, la DGI ajoute qu'il ne saurait, dans un arrêté, être préjugé des dérogations législatives ou réglementaires qui existent ou qui pourraient être instaurées. Il en est ainsi des reports d'amortissements ou de déficits dont l'origine doit pouvoir être justifiée dès lors qu'ils ont un effet sur les résultats d'un exercice non prescrit. En tout état de cause, l'administration considère que l'observation de la durée moyenne des effets des dispositions légales en vigueur permet d'indiquer que le délai maximal de conservation sera de dix ans, conformément aux articles L. 170 et L. 186 du livre des procédures fiscales.

La Commission estime cependant qu'en l'absence de tout système garantissant que les services gestionnaires informeront en temps utile les CRI des informations qui doivent être conservées au-delà du délai de deux ans, il peut raisonnablement être envisagé que l'ensemble des informations sera conservé selon les mêmes modalités pendant 10 ans. Or, la Commission s'est toujours référée aux délais légaux usuels pour apprécier la durée de conservation des informations fiscales et non à des dispositions dérogeant largement du droit commun et d'application peu fréquente.

En conséquence, la Commission considère qu'il convient que les informations restent consultables en ligne par les services fiscaux pendant deux années, conformément au délai prévu à l'article R 196-1, et qu'elles soient, ensuite, intégrées aux archives intermédiaires des CRI pendant une période ne pouvant excéder dix ans à compter de l'année d'imposition. Pendant cette période, les informations pourront être communiquées aux services des impôts qui en feront la demande. Le premier alinéa de l'article 4 du projet d'arrêté régissant le traitement « TDFC » devra être modifié en ce sens.*

En ce qui concerne les garanties apportées aux adhérents à la téléprocédure, notamment en cas de dysfonctionnement du système :

Le calendrier des obligations déclaratives subit certains aménagements pour les adhérents à la procédure « TDFC », un délai supplémentaire de 15 jours à compter de la date légale du dépôt papier leur étant systématiquement accordé, auquel s'ajoute un délai supplémentaire, accordé en cas de documents ayant fait l'objet d'un rejet technique de la part du CRI de Nevers.

Le partenaire EDI et le contribuable sont informés des suites du transfert électronique : le contribuable adhérant à TDFC reçoit, à sa demande, un accusé de réception postal relatif aux documents reçus par le CRI de Nevers. Le partenaire EDI reçoit, pour sa part, en premier lieu, un accusé de réception magnétique précisant, pour les fichiers rejetés, la nature de l'anomalie la plus grave affectant la transmission, en second lieu, un document de synthèse établi sur papier, appelé « état qualité », qui présente l'ensemble des anomalies constatées dans la transmission.

Par ailleurs, de l'émetteur initial au récepteur final (le centre ou la recette des impôts), plusieurs intermédiaires interviennent pour que la déclaration parvienne à temps au centre des impôts les centres relais, le CRI de Nevers, les opérateurs de télécommunication) et a défaillance à l'un ou l'autre de ces niveaux peut aboutir à des mises en demeure intempestives. Afin de réduire ce risque, l'administration prévoit la réduction des délais de transfert des informations des CRI vers les centres des impôts, la création de blocages logiciels à l'émission des mises en demeure lorsqu'une déclaration a été télétransmise

au CRI de Nevers, ainsi que la mise en place d'une structure départementale ayant pour mission de procéder, pour chaque incident, à un suivi personnalisé et à une analyse.

La Commission considère qu'il convient également que les documents transmis via « TDFC » fassent l'objet d'un marquage informatique spécifique à la réception des mêmes documents sur support papier, afin d'éviter toute erreur sur la nature des informations à prendre en compte pour le calcul de l'impôt.

Au bénéfice de ces déclarations, la Commission :

Émet un avis favorable sur le projet de décret et les deux projets d'arrêtés qui lui sont soumis par le ministère de l'Économie, des Finances et de l'Industrie, SOUS RÉSERVE :

— qu'une solution juridiquement satisfaisante soit trouvée à la question du support juridique de la procédure d'habilitation mise en place pour les can didats au titre de partenaire EDI,

— que, jusqu'à la mise en place de ce dispositif de cryptage dont la Com mission souhaite qu'il intervienne dans les meilleurs délais, les contribuables adhérents à « TDFC » soient clairement informés de ce que les données fisca les et comptables sont transmises en clair entre le partenaire EDI et la DGI et que seule la signature électronique fait l'objet d'un procédé de chiffrement garantissant l'origine et l'intégrité des informations, mais non leur confiden tialité,

— que les informations issues de « TDFC » soient consultables en ligne par les services fiscaux pendant deux années, qu'elles soient ensuite intégrées aux archives intermédiaires des CRI pendant une période ne pouvant pas ex céder dix ans à compter de l'année d'imposition et que le premier alinéa de l'article 4 du projet d'arrêté « TDFC » soit modifié en ce sens,

— que les documents transmis via « TDFC » fassent l'objet d'un marquage informatique spécifique à la réception des mêmes documents sur support pa pier.

Délibération n° 00-036 du 4 juillet 2000 relative à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 et à un projet d'arrêté concernant le transfert à la commission d'indemnisation des victimes de spoliations du fichier constitué par la mission d'étude sur la spoliation des personnes considérées comme juives.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le Premier ministre :

— d'un projet de décret pris en application des dispositions du troisième ali néa de l'article 31 de la loi du 6 janvier 1978 et relatif au transfert du fichier constitué par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy à la Commission pour l'indemnisa tion des victimes de spoliations intervenues du fait des législations antisémi tes en vigueur pendant l'Occupation,

— et d'un projet d'arrêté déterminant les conditions de ce transfert.

Vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 oc tobre 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, et notamment son article 31 ;

Vu le décret n° 97-1174 du 23 décembre 1997 portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 au fichier mis en œuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy ;

Vu l'arrêté du 23 décembre 1997 portant création d'un traitement automatisé d'informations nominatives mis en oeuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy, modifié par l'arrêté du 28 juillet 1999 ;

Vu le décret n° 99-778 du 10 septembre 1999 instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation ;

Après avoir entendu Monsieur Didier GASSE, commissaire en son rapport et Madame Charlotte-Marie PITRAT, commissaire du gouvernement en ses observations ;

Formule les observations suivantes :

Sur le projet de décret :

Le décret susvisé du 23 décembre 1997 avait permis la création d'un fichier qui avait pour objectif de faire un inventaire des spoliations subies pendant l'Occupation par les personnes considérées comme juives par les autorités de Vichy. S'agissant de la collecte et du traitement d'informations faisant apparaître directement ou indirectement l'origine de personnes résidant en France, considérées comme juives par les autorités de Vichy, ce décret avait été pris en application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 sur avis conforme de la Commission, compte tenu du motif d'intérêt public qui s'attachait à la mise en œuvre d'un tel fichier par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy.

Le projet de décret prévoit le transfert du fichier constitué sous l'empire du décret de 1997 à la Commission pour l'indemnisation des victimes de spoliations instituée par le décret susvisé du 10 septembre 1999.

L'objectif poursuivi est double, puisqu'il consiste, d'une part, à permettre l'indemnisation du préjudice subi par les victimes de spoliations intervenues du fait des législations antisémites et, d'autre part, à ouvrir aux associations répondant aux critères fixés par l'article 2-4 du code de procédure pénale l'accès aux données nominatives dans le cadre des recommandations relatives au « devoir de mémoire » faites par la mission d'étude sur la spoliation. Ces deux finalités, qui interviennent dans le prolongement de la création du fichier autorisé en 1997 et concernent sa mise en œuvre, relèvent bien de l'intérêt public.

La procédure suivie pour habiliter les représentants des associations est très spécifique, les autorisations d'accès étant subordonnées à la conclusion

préalable de conventions entre les associations demanderesses et les services du Premier ministre.

Sur le projet d'arrêté :

Les catégories d'informations appelées à figurer dans le traitement informatique, qui sera transféré par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy à la commission d'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation, sont relatives, s'agissant des personnes spoliées, à leur nom, prénom, adresse, profession, date et lieu de naissance, nationalité, fichage éventuel, nom et prénom des membres de la famille, nom et prénom des personnes qui se sont éventuellement déclarées comme ayants droit à la Libération, sort de la personne et des membres de la famille pendant et après la guerre.

Les informations relatives aux biens dont les propriétaires ont été dépossédés, que ces biens aient été mis sous séquestre ou administrés par des tiers, sont les nom et qualité des dépositaires et administrateurs provisoires et les opérations effectuées sur les biens par les dépositaires et administrateurs provisoires.

Les informations sur les restitutions opérées après la guerre sont relatives à l'identité des personnes ayant réclamé le bien, ainsi que des personnes appelées à le restituer.

Les informations nominatives faisant l'objet de ce traitement font apparaître que les personnes concernées ont été considérées comme juives par les autorités de Vichy, un projet de décret pris en application du troisième alinéa de l'article 31 de la loi au 6 janvier 1978 autorisant la collecte et le traitement de telles données étant soumis simultanément à l'appréciation de la Commission.

Les destinataires des informations nominatives traitées seront les membres de la commission d'indemnisation, son directeur, son rapporteur général, ses rapporteurs ; les personnes travaillant pour son compte et sous son autorité sont habilitées à consulter le fichier par décision du président de la commission. L'arrêté rappelle qu'ont également accès aux données du fichier les personnes désignées par les associations agréées en application du décret susvisé, dans les formes et selon les conditions prévues en son article 2 ;

Le droit d'accès prévu au chapitre V de la loi n ? 78-17 du 6 janvier 1978 s'exerce auprès du président de la commission d'indemnisation.

Compte tenu de ces observations, la Commission :

Émet un avis conforme au projet de décret tel qu'il a été soumis par le Premier ministre,

Émet un avis favorable au projet d'arrêté présenté par le Premier ministre sous réserve que le projet de décret, pris en application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 et pour lequel un avis conforme a été donné par la présente délibération soit préalablement ou simultanément publié au Journal officiel.

Délibération n° 00-037 du 4 juillet 2000 portant avis sur un projet d'arrêté modifiant l'arrêté du 18 juin 1999 présenté par le ministère de la Justice relatif à un modèle-type de traitement concernant le suivi des affaires pénales du parquet général des cours d'appel.

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de la Justice d'un projet d'arrêté modifiant l'arrêté du 18 juin 1999 portant création d'un modèle-type de traitement automatisé d'informations nominatives à caractère personnel relatif à la gestion du suivi des affaires pénales par le parquet général des cours d'appel,

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 les articles 34 à 38 du code de procédure pénale ;

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

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

Vu le décret n° 90-115 du 2 février 1990 portant application aux juridictions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 précitée ;

Vu l'arrêté du Garde des Sceaux du 18 juin 1999 ;

Vu la délibération de la CNIL n° 99-29 du 4 mai 1999 ;

Vu le projet d'arrêté présenté par le Garde des Sceaux, ministre de la Justice ;

Après avoir entendu Monsieur Gérard Gouzes, vice-président, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

Le projet d'arrêté modificatif dont est saisie la Commission a pour objet de supprimer de la liste des informations nominatives appelées à figurer dans le traitement et énumérées à l'article 3 de l'arrêté du 18 juin 1999, les informations concernant les avoués, avocats, huissiers, notaires, experts judiciaires, mandataires de justice, magistrats consulaires.

Il prévoit également une nouvelle rédaction de l'article 4 de l'arrêté afin de préciser que les seuls destinataires des informations enregistrées dans le traitement sont les magistrats et fonctionnaires habilités du parquet général.

Le projet introduit par ailleurs une modification de l'article 3 de l'arrêté du 18 juin 1999 pour remplacer la notion de personnes « mises en cause » dans une enquête préliminaire ou de flagrance, par celle de personnes « visées par » une telle procédure et une modification de rédaction de la première phrase de l'article 7 précisant que les informations nominatives « sont conservées pendant une durée égale aux délais légaux de prescription de la peine mais n'excédant pas cinq ans à compter du jour où la dernière décision est devenue définitive avec mise à jour en cas d'amnistie ou de réhabilitation ».

Les modifications envisagées n'appellent pas d'observations au regard des dispositions de la loi du 6 janvier 1978. Par suite, la Commission :
Émet un avis favorable au projet d'arrêté modificatif soumis par le Garde des Sceaux, ministre de la Justice.

Délibération n° 00-038 du 4 juillet 2000 portant avis sur l'utilisation, par l'INSEE, du fichier de la taxe d'habitation en vue des prochains recensements de population.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté concernant l'exploitation automatisée du fichier de la taxe d'habitation ;

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

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

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Vu l'arrêté du 8 mars 1996 régissant le traitement automatisé de la taxe d'habitation à la direction générale des Impôts ; Vu le projet d'arrêté portant création du traitement ;

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 :

Sur *la finalité du traitement*

La Commission est saisie par l'INSEE d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé d'informations nominatives qui a pour finalité l'exploitation des données issues du fichier de la taxe d'habitation (F.T.H.) de 1999.

L'objectif du traitement est l'étude des écarts existant, en ce qui concerne les logements, entre les résultats du recensement général de la population de 1999 et les données issues de la taxe d'habitation 1999 ainsi que l'utilisation des fichiers de la taxe d'habitation (F.T.H.) dans certaines phases du recensement rénové de population.

La Commission relève que cette mise à disposition de l'INSEE des données des F.T.H. est effectuée conformément aux dispositions de l'article 5 de l'arrêté susvisé de mars 1996.

Sur la nature des informations enregistrées

Les informations traitées sont les suivantes : le code département, code INSEE commune (avec arrondissement pour Paris, Lyon, Marseille), le libellé de voie ou lieu-dit, le code RIVOLI, la section cadastrale, le numéro de voie, l'indice de répétition (pour bis, ter, quater...), le bâtiment, l'escalier, le niveau, le code local, le nombre de pièces habitables, le code affectation (habitation, mixte — habitation et professionnelle), le code occupation (propriétaire, locataire, occupant à titre gratuit, bail rural, local vacant, local meublé), le code taxation (résidence principale, résidence secondaire), le nom de l'occupant.

La Commission considère que ces données sont pertinentes, adéquates et non excessives au regard de la finalité poursuivie en l'espèce. Elle relève que les fichiers seront rendus anonymes par l'INSEE à compter de juin 2001.

Sur les destinataires des informations

Seuls les agents habilités de l'INSEE, soumis au respect du secret statistique, auront connaissance des informations et documents nominatifs établis lors de ce traitement. Aucune information de nature à compléter le fichier de la taxe d'habitation ne sera communiquée à la direction générale des Impôts.

Sur l'exercice du droit d'accès

Le droit d'accès et de rectification prévu par l'article 34 de la loi n° 78-17 du 6 janvier 1978, s'exercera auprès de la direction générale de l'INSEE.

Compte tenu de ces observations, la Commissions :

Émet un avis favorable au projet d'arrêté qui lui est présenté.

Délibération n° 00-039 du 4 juillet 2000 portant avis sur la mise en place, par l'INSEE, d'un répertoire des immeubles localisés (R.I.L.)

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le directeur général de l'INSEE d'un projet d'arrêté concernant la création d'un traitement automatisé d'informations nominatives qui a pour finalité la création et la mise à jour d'un répertoire d'immeubles localisés (R.I.L.) ;

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

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

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Vu le projet d'arrêté portant création du traitement ;

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 :

Sur la finalité du traitement

La Commission est saisie par l'INSEE d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé d'informations nominatives qui a pour finalité la création et la mise à jour d'un répertoire d'immeubles localisés (R.I.L).

Ce répertoire doit permettre d'améliorer et de préciser le système d'information géographique central de l'INSEE.

Sur la nature des informations traitées

Les informations enregistrées dans le répertoire d'immeubles localisés ont trait à :
— l'adresse : coordonnées géographiques, type et nom de la voie, numéro dans la voie, date de création de l'adresse, indication de son fichier d'origine et de sa mise à jour ;
— l'immeuble : type d'immeuble (immeuble d'habitation, d'activités, d'équipement urbain, mixte), âge, date d'entrée dans le R.I.L., date de destruction et de dernière modification, nombre de logements, nombre d'étages, nombre de communautés, nombre d'établissements, type d'équipement urbain.

La Commission relève que les données traitées sont pertinentes, adéquates et non excessives au regard de la finalité poursuivie, et qu'aucune donnée identifiant les personnes physiques habitant les immeubles référencés ne figurera dans le R.I.L.

Sur la constitution et la mise à jour du R.I.L

La constitution initiale du R.I.L. est effectuée à partir de la cartographie numérisée établie pour le recensement général de la population (RGP) de 1999 ainsi que des données issues des bordereaux de district du RGP 1999.

Sa mise à jour est réalisée à partir des fichiers de permis de construire et de démolir, du répertoire des entreprises et de leurs établissements (SIRENE), ainsi que de fichiers administratifs comportant une adresse dont l'INSEE est destinataire en application de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 modifiée.

Le R.I.L. est exclusivement destiné à l'INSEE.

Le droit d'accès et de rectification prévu par l'article 34 de la loi n° 78-17 du 6 janvier 1978 s'exerce auprès de l'INSEE.

Compte tenu de ces observations, la Commission :

Émet un avis favorable au projet d'arrêté présenté.

Délibération n 00-040 du 4 juillet 2000 relative à une demande d'avis sur un projet de décret relatif à la transposition en droit français des directives 97/66/CE et 98/10/CE et modifiant le code des postes et télécommunications

La Commission nationale de l'informatique et des libertés, Saisie pour avis par le secrétaire d'État le 20 juin 1999 d'un projet de décret relatif à la transposition en droit français des directives 97/66/CE et 98/10/CE et modifiant le code des postes et télécommunications,

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 concernant 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 directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ;

Vu la directive 98/10/CE du Parlement européen et du Conseil concernent l'application de la fourniture d'un réseau ouvert (ONP) à la téléphonie vocale et l'établissement d'un service universel des télécommunications dans un environnement concurrentiel ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le décret V78-774 du 17 juillet modifié pris pour l'application de la loi précitée ;

Vu la loi V96-659 du 26 juillet 1996 de réglementation des télécommunications, ensemble le décret V96-1225 du 27 décembre 1996 portant approbation du cahier des charges de France Télécom et le décret V96-1175 du 27 décembre 1996 relatif aux clauses types des cahiers des charges associés aux autorisations attribuées en application des articles L. 33-1 et L. 34-1 ;

Vu la décision du Président du conseil d'administration de France Télécom portant création d'un traitement automatisé concernant la base de données annuaires de France Télécom en date du 23 janvier 1998 prise après avis de la Commission ;

Vu la délibération V99-048 du 14 octobre 1999 portant adoption du rapport relatif au publipostage électronique et la protection des données personnelles ;

Vu la délibération n°00-009 du 27 janvier 2000 portant avis sur un projet de loi relatif à diverses dispositions d'adaptation communautaire ;

Vu le courrier adressé le 12 juillet 1999 par le Président de la CNIL au directeur général de l'Industrie, des Technologies de l'Information et des Postes sur un avant-projet de décret destiné à la transposition des directives 97/66/CE et 98/10/CE,

Après avoir entendu Monsieur Marcel Pinet en son rapport et Madame Charlotte-Marie Pitrat en ses observations,

Présente les observations suivantes, au soutien des avis qu'elle formule ci après :

/ — La Commission constate avec satisfaction qu'un nombre important des observations qu'elle avait formulées le 12 juillet 1999 sur un avant-projet de décret ont été prises en considération.

Ainsi :
— la liste des données pouvant être conservées pour les besoins de factura tion prévue à l'article D. 98.12 du c) 4e alinéa, du code des PetT a été com plétée, dans un souci de transparence, par la mention du lieu de l'appel ;
— la contradiction relevée en matière d'exploitation des données de factu ration à des fins de commercialisation des services de télécommunication de l'opérateur, résultant du maintien, à côté d'une disposition exigeant, confor mément à l'article 6, paragraphe 3 de la directive 97/66/CE, le consente ment de l'abonné pour de telles opérations, d'une autre disposition exigeant un simple droit d'opposition de la personne concernée, a été levée par la suppression de cette mention ;
— l'ambiguïté relevée sur la portée du droit d'opposition qui paraissait can tonné à la seule offre du service par l'opérateur de l'abonné (alors que ce service pouvait être mis en œuvre également par un autre opérateur) a été levée ;
— au 11e paragraphe du 2 du c) de l'article D 98-1, une nouvelle option en matière de présentation du numéro appelant a été établie, permettant gratui tement et simplement la levée ponctuelle du secret permanent demandé par l'abonné en matière de présentation du numéro appelant ; cette option per met, en effet, aux abonnés de ne pas renoncer à l'option du secret perma nent, prévue par ailleurs, tout en les laissant en mesure d'autoriser ponctuellement l'opérateur à transmettre leur numéro lorsqu'ils le souhaitent ou lorsqu'un service ou un correspondant en exige la présentation pour des motifs légitimes ;
— le droit pour toute personne de ne pas être mentionnée sur les listes d'abonnés ou d'utilisateurs publiés, est opposable également aux services des renseignements téléphoniques en ce qu'ils sont désormais visés à l'ar ticle 1 du projet de décret modifiant l'article D. 98-1, I, 2, c), deuxième ali néa, premier tiret ;
— l'obligation des opérateurs d'informer leurs abonnés sur leurs droits en matière de présentation du numéro de la ligne appelante a été établie.

// — La Commission demeure cependant préoccupée sur plusieurs points.

1 — Les listes d'abonnés (annuaires)

a) La gratuité de la « liste rouge » souhaitée de manière constante par la Commission n'est pas instituée.

b) La gratuité du droit ne pas figurer sur les listes d'abonnés mis en ligne sur Internet qui est de droit en ce qui concerne l'annuaire de France Télécom de puis la publication de sa décision relative aux services d'annuaires prise après avis de la CNIL (délibération n° 98-001 du 13 janvier 1998, décision de France Télécom du janvier 1998, JO du 20 février 1998) n'est pas non plus prévue. Or, la publication des annuaires étant libre, rien n'empêche un autre opérateur de procéder à la mise en ligne sur Internet d'annuaires de té-

lécommunication. Dès lors le droit de demander gratuitement à ne pas figurer sur ces annuaires devrait être consacré.

c) Le droit de s'opposer à figurer dans les annuaires inversés n'est pas prévu. Les services d'annuaires inversés ne sont pas visés par la réglementation communautaire. Néanmoins, outre l'existence des services d'annuaires inversés offerts par France Télécom à l'égard duquel la réglementation prévoit un droit d'opposition à y figurer, deux autres services d'annuaires inversés privés existent qui sont accessibles par minitel ou sur CD ROM.

Dans ces circonstances, la Commission est d'avis que le projet de décret doit être modifié de la manière suivante :

— ajouter à la fin du premier tiret du deuxième alinéa, deuxième phrase du 2 du c) de l'article D. 98-1, le membre de phrase suivant :

« ... ; *la gratuité de cette faculté est de droit lorsque les listes d'abonnés sont accessibles par les réseaux ouverts ou sont diffusées sur CD ROM ».*

— insérer le tiret supplémentaire suivant après le deuxième tiret du deuxième alinéa du 2 du c) de l'article D. 98-1 :

« En particulier l'opérateur garantit le droit de toute personne

— de *s'opposer gratuitement à être mentionnée dans les listes d'abonnés in versées publiées sur quelque support que ce soit ou accessibles par un ser vice de renseignement téléphonique qui permettent d'obtenir le nom et l'adresse d'une personne à partir de l'indication de son numéro de télé phone «*

2 — La prospection par utilisation de données issues de listes d'abonnés

L'article 1 du projet de décret modifiant l'article D 98-1, 2, c) quatrième tiret prévoit le droit d'opposition en matière d'utilisation des données issues des listes d'abonnés dans des opérations « commerciales » par voie postale ou « par voie de télécommunication ».

Les expressions « opérations commerciales » et « par voie de télécommunication » ne tiennent pas compte du projet de loi sur lequel la Commission a rendu l'avis n° 00-009 du 27 janvier 2000, et des articles 11 et 12 de la directive 97/66 qui, d'une part, visent toute opération de prospection directe quelle qu'en soit la nature et, d'autre part, prévoit non le droit d'opposition mais le consentement préalable des personnes concernées en matière de prospection par automates d'appel ou par télécopie. Par ailleurs, l'expression « par voie de télécommunication » laisse peser une ambiguïté à l'égard à la prospection par messagerie électronique lorsque l'adresse de courrier électronique figure sur une liste d'abonnés publiée. Cette donnée appelle en effet une protection particulière en ce qu'elle ne devrait figurer sur les listes d'abonnés publiées qu'à la demande des intéressés en tant qu'information « supplémentaire », ainsi que le prévoit l'article 11 de la directive 97/66, et ne pas pouvoir être utilisée dans des opérations de prospection directe du seul fait qu'elle est rendue ainsi publique.

Pour toutes ces raisons, la Commission est d'avis qu'il y a lieu de modifier et compléter la rédaction du texte relatif aux droits des abonnés en matière de prospection prévus à l'article D 98-1, 2, c, deuxième alinéa, quatrième tiret en la développant selon les quatre libellés suivants :

« L'opérateur garantit le droit de toute personne

(tiret 4) — d'interdire gratuitement que *les données à caractère personnel* la concernant issues des listes d'abonnés *ou d'utilisateurs* soient utilisées dans les opérations *de prospection directe* par voie postale, par voie *d'appel téléphonique passé par un opérateur humain* ou par voie de télécommunication à l'exception des opérations concernant l'activité autorisée relevant de la relation contractuelle entre l'opérateur et l'abonné ;
(tiret 4 bis) — *de ne pas être l'objet d'une prospection directe par voie d'automate d'appel ou de télécopie sans son consentement préalable* « (tiret 4 ter) — de *ne voir figurer que de manière volontaire son adresse électronique de courrier électronique sur les listes d'abonnés ou d'utilisateurs publiées sur quelque support que ce soit ;*
(tiret 4 quater) — de *ne pas être l'objet d'une prospection par messagerie électronique à partir de l'adresse électronique qu'elle aura demandé de faire figurer, le cas échéant, sur les listes d'abonnés ou d'utilisateurs publiées sous quelque forme que ce soit lorsque qu'une telle possibilité lui est offerte ;*

3 — L'information des abonnés et des utilisateurs sur leurs droits lors de la souscription de l'abonnement

La Commission rappelle qu'en l'absence d'une information appropriée et complète, les abonnés et les utilisateurs des réseaux de télécommunications ne sont pas en mesure d'exercer véritablement les droits qui leur sont reconnus compte tenu notamment de l'évolution rapide des services nouveaux.

C'est pourquoi, en vertu du principe de la loyauté de la collecte et du traitement des données, et compte tenu du caractère nouveau de certains des droits visés par le décret, qui sont attachés soit au traitement d'informations très sensibles, tel que l'exploitation par l'opérateur à des fins de commercialisation de ses services, des données relatives au détail de la facture, soit à la communication à des tiers de données (annuaire, commercialisation des données issues des annuaires, annuaires inversés, annuaire Internet ou sur CD ROM, présentation du numéro appelant), dont les abonnés sont susceptibles d'ignorer l'existence, la Commission estime que toute personne devrait être informée de ses droits au moment de la souscription d'un abonnement et que les abonnés actuels devraient être informés individuellement des droits qui leur sont reconnus et dont ils n'auraient pas été antérieurement informés.

◦ cette fin, la Commission est d'avis qu'il y a lieu de compléter le projet de décret en :
— ajoutant l'alinéa suivant après le 16e alinéa de l'article D. 98-2 du c)
« L'opérateur informe individuellement ses abonnés, préalablement à la souscription du contrat, des droits dont ils disposent visés aux alinéas 2, 5, 6, 10 à 16 » (selon la numérotation actuelle du projet de décret soumis)
— ajoutant à l'article 5 du projet de décret un troisième alinéa
« Les *opérateurs informent individuellement les abonnés concernés de tout droit visé aux alinéas 2, 5, 6, 10 à 16 qui n'aurait pas été antérieurement porté à leur connaissance* (selon la numérotation du projet de décret soumis) »

4 — Mise à jour du texte

La Commission signale que la rédaction du deuxième alinéa de l'article 5 du projet de décret comporte une erreur matérielle en visant non le sixième alinéa du 2 du c) de l'article D. 98-1 (selon la numérotation du projet de décret qui lui est soumis) relatif à l'information des abonnés actuels sur leur droit

d'opposition à l'exploitation par l'opérateur des données de détail de facturation à des fins de commercialisation de ses service, mais le cinquième alinéa.

5-Terminologie

Par souci de cohérence avec la terminologie utilisée tant dans les directive 95/46/62 et 97/66/62 que dans le projet de loi modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission recommande qu'en lieu et place de l'expression « informations identifiantes », l'expression « données à caractère personnel » soit utilisée aux quatrième et cinquième tirets du deuxième alinéa du 2 du c) de l'article D. 98-1.

En conclusion de tout ce qui précède, la Commission :

Emet un avis favorable sur le projet de décret au bénéfice des observations énoncées ci dessus.

Délibération n° 00-041 du 21 septembre 2000 portant avis *sur* un projet de disposition législative relative à la création d'un répertoire national des retraites et des pensions et d'un échantillon inter-régimes de cotisants.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le directeur de la sécurité sociale d'un projet de disposition législative appelée à figurer dans le pro et de la loi de financement de la sécurité sociale et relative respectivement à a création d'un répertoire national des retraites et des pensions et à l'établissement d'un échantillon inter-régimes de cotisants ;

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

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

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

Après avoir entendu Monsieur Maurice VIENNOIS, commissaire en son rapport, et Madame Charlotte-Marie PITRAT, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministère de l'Emploi et de la Solidarité a saisi la Commission, pour avis, d'une disposition appelée à figurer dans le projet de la loi de financement de la sécurité sociale pour 2001 et relative respectivement à la création d'un répertoire national des retraites et des pensions et à l'établissement d'un échantillon inter-régimes de cotisants (futur article L 161-17.1 du code de la sécurité sociale) ;

Sur le répertoire national des retraites et des pensions :

Aux termes du projet de disposition soumis à la Commission, le répertoire national des retraites et des pensions aurait pour fins « d'améliorer la connaissance statistique sur les effectifs de retraités et les montants des retraites et de faciliter la coordination entre les régimes de retraite en matière de service des prestations » ;

Selon le Ministère, la création du répertoire pourrait en effet remédier aux insuffisances du système d'information statistique actuel qui, reposant essentiellement sur l'exploitation de l'échantillon statistique inter-régimes des retraites institué par la loi du 9 juillet 1984, ne permet de connaître ni le nombre de retraités, compte tenu des doubles comptes multiples entre les régimes, ni la composition des revenus de retraites. La mise en place du répertoire permettrait en outre de disposer des statistiques nécessaires pour assurer le calcul des compensations financières entre les différents régimes de retraites.

La Commission relève que la poursuite de cette finalité statistique est légitime mais qu'elle ne saurait justifier à elle seule la constitution d'un fichier national nominatif. Elle observe toutefois que le répertoire a également pour finalité d'assurer une meilleure coordination entre régimes en permettant notamment de mieux appliquer les règles de cumul des pensions et de limiter les versements indus.

En effet, la connaissance actuelle par les organismes de retraite, de ces situations, repose essentiellement sur les déclarations des intéressés qui, compte tenu de la complexité des règles en vigueur et de la difficulté pour les personnes concernées d'appréhender parfaitement ces règles, ne sont pas jugées fiables.

La communication systématique, par les organismes débiteurs d'avantages de retraite, de la nature et du montant des avantages servis permettrait, par rapprochement de ces informations dans le répertoire, de détecter les situations de cumuls éventuels et d'en informer en conséquence les caisses de retraite concernées, à charge pour elles de vérifier les cas de cumuls ainsi constatés et d'éviter ainsi le versement d'indus.

Cette seconde finalité de contrôle qui justifie en conséquence l'enregistrement, dans le répertoire, des informations nécessaires à l'identification des personnes bénéficiaires d'avantages de retraite devrait être explicitement mentionnée au premier alinéa du paragraphe I du futur article L 161-17-1 du code de la sécurité sociale.

Le projet de disposition prévoit que le numéro d'inscription au répertoire national d'identification des personnes physiques sera utilisé dans les traitements et échanges d'informations mis en œuvre par les organismes débiteurs d'avantages de retraite.

La Commission relève à cet égard que ces organismes ont été autorisés, en application des articles R 115-1 et R 115-2 du code de la sécurité sociale (décret du 3 avril 1985 abrogé et remplacé par le décret du 12 septembre 1996, pris après avis favorables de la Commission) à utiliser ce numéro dans leurs traitements.

Elle estime qu'eu égard au caractère exhaustif et national du fichier qui serait ainsi constitué et à la présence du NIR dans ce fichier, sa mise en œuvre doit être entourée de dispositifs particuliers de sécurité et qu'en particulier,

des mesures de destruction éventuelles doivent être prévues en cas de survenue de circonstances exceptionnelles.

Ces mesures devraient être fixées par le décret qui, prévu au dernier alinéa du paragraphe II, déterminera le contenu et les modalités de gestion et d'utilisation du répertoire. Ce décret sera pris après avis de la CNIL.

Sur l'échantillon statistique inter-régimes des cotisants :

Le projet de disposition législative soumis à la commission prévoit également la création d'un échantillon statistique inter-régimes de cotisants, anonyme et représentatif, visant à élaborer un système d'information sur les droits acquis à la retraite par les personnes d'âge actif.

Cet échantillon serait élaboré à partir des informations fournies par les différents organismes débiteurs d'avantages de retraite et permettrait d'évaluer la situation des personnes d'âge actif au regard de leurs droits futurs à retraite et en particulier d'apprécier, de façon permanente, l'acquis résultant des carrières effectuées ainsi que les ruptures éventuelles dans ces carrières.

La Commission relève avec intérêt, qu'aux termes du projet de disposition législative, l'échantillon sera anonyme et qu'un décret pris après avis de la CNIL fixera les conditions de communication des données.

Ainsi, la Commission sera en mesure d'apprécier les dispositions effectivement prises pour assurer l'anonymat des données.

Elle considère à cet égard qu'il conviendrait que le décret détermine également les modalités de fixation de l'échantillon.

Elle estime dès lors qu'il y a lieu de supprimer le dernier alinéa du paragraphe II de cette disposition qui prévoit que l'élaboration de ce système d'information serait soumise à la procédure prévue à l'article 15 de la loi du 6 janvier 1978. Compte tenu de ces observations, la commission est d'avis :

— que les finalités de contrôle des situations de cumuls des avantages de re traite soient précisées au premier alinéa du paragraphe I du futur article L 161-17-1 du code de la sécurité sociale ;

— que le dernier alinéa du paragraphe I du futur article L 161-17.1 du code de la sécurité sociale soit rédigé ainsi : « le contenu, les modalités de gestion et d'utilisation de ce répertoire *ainsi que les dispositions prévues pour assurer la sécurité des informations,* sont fixées par décret en Conseil d'État, après avis de la CNIL » ;

— que l'avant dernier alinéa du paragraphe II du futur article L 161-17-1 du code de la sécurité sociale soit rédigé ainsi : « un décret, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les conditions de communication des données mentionnées au premier alinéa et *les modalités de fixation de l'échantillon* » ;

— que le dernier alinéa du paragraphe II du futur article L 161-17.1 du code de la sécurité sociale soit supprimé.

Délibération n° 00-042 du 21 septembre 2000 relative à un projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 au fichier mis en œuvre par la commission pour l'indemnisation des victimes de spoliations

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le Premier ministre d'un projet de décret portant application des dispositions du troisième alinéa de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 au fichier mis en œuvre par la commission pour l'indemnisation des victimes de spoliations,

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, et notamment son article 31 ;

Vu le décret n 97-1174 du 23 décembre 1997 portant application des dispositions du troisième alinéa de l'article 31 de la loi n ? 78-17 du 6 janvier 1978 au fichier mis en œuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy ;

Vu l'arrêté du 23 décembre 1997 portant création d'un traitement automatisé d'informations nominatives mis en œuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy, modifié par l'arrêté du 28 juillet 1999 ;

Vu le décret n° 99-778 du 10 septembre 1999 instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation, modifié par le décret n 99-914 du 27 octobre 1999 ;

Vu la délibération n° 00-36 du 4 juillet 2000 relative à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 et à un projet d'arrêté concernant le transfert à la commission d'indemnisation des victimes de spoliations du fichier constitué par la mission d'étude sur la spoliation des personnes considérées comme juives.

Après avoir entendu monsieur Didier GASSE, commissaire en son rapport et Madame Charlotte-Marie PITRAT, commissaire du gouvernement en ses observations ;

Formule les observations suivantes :

Par la délibération susvisée, la Commission a donné un avis conforme au projet de décret qui lui avait été soumis par le Premier ministre aux fins de permettre le transfert du fichier de la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy à la commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation.

Le nouveau projet qui lui est soumis, à la suite de son examen par le Conseil d'État, section de l'Intérieur, a notamment pour objet, outre quelques modifi-

cations d'ordre rédactionnel, d'une part, de préciser que l'autorisation accordée à la commission instituée par le décret du 10 septembre 1999 susvisé, dans le cadre de l'examen des demandes individuelles présentées par les victimes ou leurs ayants droit pour la réparation des préjudices consécutifs aux spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation, vise la collecte et le traitement des informations faisant apparaître, directement ou indirectement, l'origine des personnes résidant en France, considérées comme juives par l'occupant ou par les autorités de Vichy et ayant subi des spoliations de ce fait et, d'autre part, de réserver, sous certaines conditions, l'accès du fichier aux seules associations, régulièrement déclarées depuis au moins cinq ans, ayant pour objet de perpétuer le souvenir des persécutions consécutives aux législations antisémites en vigueur pendant l'Occupation ou de défendre les intérêts matériels et moraux des personnes mentionnées à l'article 1er du décret du 10 septembre 1999.

Ce projet, en cet état, n'appelle pas d'observation particulière.

La Commission croit cependant utile de faire observer que le deuxième alinéa de l'article 2 du projet pourrait préciser que la convention d'autorisation d'accès de ces associations est conclue « par le Premier ministre ».

La commission émet un avis conforme au nouveau projet de décret qui lui est soumis par le Premier ministre.

Délibération n° 00-043 du 3 octobre 2000 concernant l'informatisation de la gestion par la direction générale des Impôts de la taxe annuelle sur les logements vacants.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le ministre de l'Economie, des Finances et de l'Industrie :
— d'un projet d'arrêté « relatif à la mise en service par la direction générale des Impôts du traitement informatisé de la taxe annuelle sur les logements va cants » (traitement « TLV »),
— d'un projet d'arrêté « modifiant l'arrêté du 25 juillet 1988 autorisant la création d'un traitement automatisé relatif à l'informatisation des inspections d'assiette et de documentation » (traitement « ILIAD »),
— d'un projet d'arrêté « modifiant l'arrêté du 5 janvier 1990 relatif à la création d'un système automatisé de gestion de l'identité et des adresses des contribuables à l'impôt sur le revenu, à la taxe d'habitation et à l'impôt de solidarité sur la fortune » (traitement « FIP »),
— d'un projet d'arrêté « modifiant l'arrêté du 8 mars 1996 régissant le trai tement informatisé de la taxe d'habitation à la direction générale des Impôts » (traitement « 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, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée,

Vu l'article 51 de la loi n° 98-657 du 29 juillet 1998 relative à la lutte contre les exclusions qui introduit un article 232 dans le code général des impôts, ensemble la décision n° 98-403 DC du 29 juillet 1999 du Conseil constitutionnel,

Après avoir entendu Monsieur Noël CHAHID-NOURAÏ en son rapport et Madame Charlotte-Marie PITRAT, commissaire du gouvernement, en ses observations,

Formule les observations suivantes :

Le traitement dénommé « TLV », qui fait l'objet de la première des demandes d'avis transmises par le ministère de l'Economie, des Finances et de l'Industrie à la Commission nationale de l'informatique et des libertés, a pour finalité d'assurer l'imposition des redevables de la taxe annuelle sur les logements vacants (TLV).

Les autres saisines pour avis se rapportent à la mise en place de nouveaux échanges d'informations consécutifs à la mise en place de la taxe, qui font intervenir trois autres traitements de la direction générale des Impôts (DGI) :

— le traitement « ILIAD », qui est utilisé par les inspections d'assiette et de documentation des centres des impôts (CDI) pour la gestion de l'impôt sur le revenu, de la taxe d'habitation, de la CSG, de la CRDS et des affaires contentieuses concernant ces impôts,

— le traitement « FIP », qui gère, pour chaque direction des services fis caux, les éléments d'état civil et les adresses des contribuables à l'impôt sur le revenu, à la taxe d'habitation et à l'impôt de solidarité sur la fortune, et qui attribue à chaque foyer fiscal un identifiant départemental FIP,

— le traitement « TH », qui assure l'imposition à la taxe d'habitation, la col lecte des éléments d'assiette et la communication des rôles aux personnes habilitées à en connaître.

/. Sur le cadre juridique du traitement

L'article 51 de la loi d'orientation du 29 juillet 1998 relative à la lutte contre les exclusions a instauré, à compter du 1er janvier 1999, une taxe spécifique annuelle dans les communes, désignées par décret, qui sont situées dans une zone d'urbanisation continue de plus de 200 000 habitants où existe un déséquilibre marqué entre l'offre et la demande de logements au détriment des personnes à faibles revenus. Sont soumis à cette taxe les détenteurs d'un logement inoccupé depuis au moins deux années consécutives, lorsque la vacance est indépendante de la volonté du contribuable. Cependant, la taxe n'est pas due pour les logements détenus par les organismes d'habitations à loyer modéré ou par les sociétés d'économie mixte et destinés à être attribués sous condition de ressources.

La loi définit l'assiette de la taxe (la valeur locative du logement), le taux d'imposition (qui varie selon la durée de la vacance), les personnes imposables (le propriétaire, l'usufruitier, le preneur à bail ou l'emphytéote), ainsi que les règles de contrôle, de recouvrement et de procédure contentieuse qui sont identiques à celles qui s'appliquent pour la taxe sur le foncier bâti.

Le Conseil constitutionnel, appelé à s'assurer de la constitutionnalité de cette disposition, a émis, dans sa décision du 29 juillet 1999, une réserve d'inter-

prétation, ainsi énoncée : « l'objet de la taxation [étant] d'inciter les personnes [qui y sont assujetties] à mettre en location des logements susceptibles d'être loués [] la différence de traitement fiscal instaurée par cet article entre [les bailleurs privés et publics et, parmi les bailleurs privés, entre les sociétés d'économie mixte de logement social et les autres propriétaires] n'est conforme à la Constitution que si les critères d'assujettissement [...] sont en rapport direct avec cet objet ; [...] ladite taxation ne peut dès lors frapper que des logements habitables, vacants et dont la vacance tient à la seule volonté de leur détenteur ».

Dans ces conditions, le Conseil constitutionnel a déclaré l'article 51 conforme à la Constitution, sous réserve d'une interprétation neutralisante, dont il résulte que « ne sauraient être assujettis » les « logements qui ne pourraient être rendus habitables qu'au prix de travaux importants et dont la charge incomberait nécessairement à leur détenteur », les « logements meublés affectés à l'habitation et, comme tels, assujettis [...] à la taxe d'habitation », les « logements dont la vacance est imputable à une cause étrangère à la volonté du bailleur, faisant obstacle à leur occupation durable, à titre onéreux ou gratuit, dans des conditions normales d'habitation, ou s'opposant à leur occupation, à titre onéreux ou gratuit, dans des conditions normales de rémunération du bailleur », les « logements ayant vocation, dans un délai proche, à disparaître ou à faire l'objet de travaux dans le cadre d'opérations d'urbanisme, de réhabilitation ou de démolition », ou les « logements mis en location ou en vente aux prix du marché et ne trouvant pas preneur ».

// résulte de ce qui précède d'une part, que le champ d'exigibilité de la taxe sur les logements vacants n'inclut pas la totalité des logements inoccupés depuis au moins deux années consécutives au 1er janvier de l'année d'imposition, mais uniquement ceux qui, répondant à ce premier critère, n'entrent dans aucune des catégories susmentionnées, d'autre part et par voie de conséquence, que la taxation ne peut pas se déduire de la seule absence d'assujettissement à la taxe d'habitation.

II. Sur les traitements automatisés mis en œuvre

Le dispositif informatique proposé prévoit que la finalité du traitement « ILIAD » des CDI est étendue à la gestion de la taxe annuelle sur les logements vacants : aide au recensement des redevables, suivi de la taxation, traitement des demandes de dégrèvement, émission des impositions supplémentaires.

En ce qui concerne le recensement des personnes assujetties à la taxe, il est prévu d'utiliser, dans un premier temps, les informations gérées par le traitement « TH » afin d'obtenir la liste des logements identifiés comme étant vacants au sens de la taxe d'habitation.

Les listes ainsi constituées sans l'intervention des CDI comprennent les logements qui sont considérés comme étant inoccupés au 1er janvier de l'année de taxation, qui ne sont pas imposés à la taxe d'habitation depuis au moins deux ans, et dont le propriétaire n'a pas changé durant cette période. Les informations recueillies à partir des traitements « TH » et « FIP » concernent l'identité du propriétaire, la valeur locative brute et l'année de vacance du logement. Elles sont transmises au traitement « TLV », en charge des opérations de taxation et de l'émission des rôles.

Toutefois, cette première sélection ne permet pas d'exclure certaines catégories de logements qui n'entrent pas dans le champ d'application de la TLV, tels que les logements qui ne sont pas habitables (non clos), ceux qui ont été occupés temporairement plus de 30 jours au cours de l'une des deux précédentes années, ceux dont la vacance trouve son origine dans la nécessité de réaliser d'importants travaux, ceux qui doivent être prochainement détruits ou encore ceux qui ne trouvent pas preneur, bien qu'étant mis en vente ou en location au prix du marché.

C'est pourquoi la DGI prévoit de mettre ces informations à la disposition des CDI, via le traitement « ILIAD », préalablement à toute taxation, afin que ces services — les mieux à même d'apprécier les situations concrètes — aient la possibilité de s'opposer, sur la base des justificatifs déjà adressés par les intéressés ou de leur connaissance du terrain, à l'assujettissement des logements au cas par cas. Les CDI ont la faculté de modifier deux informations au sein du fichier « ILIAD », en vue de leur communication au traitement « TLV » :
— l'indication de la vacance du logement au sens de la taxe d'habitation,
— l'année à partir de laquelle sera décomptée la période de référence de la taxe, qui servira pour déterminer l'année où le logement sera potentielle ment imposable.

Cependant, dès lors que les CDI ne disposent pas, au titre de la gestion d'une autre imposition, de l'ensemble des éléments factuels pertinents pour identifier les personnes qui entrent dans le champ d'application de la TLV, seule la collecte, dès avant l'émission des rôles de la TLV et l'envoi des avis d'imposition, d'informations complémentaires auprès des personnes susceptibles d'être concernées au vu des listes transmises par l'application « TH » est de nature à éviter d'imposer à la taxe des contribuables qui ne répondraient pas aux critères de taxation posés par la loi.

La Commission prend acte de ce qu'en conséquence, la DGI prévoit l'envoi, dans un délai raisonnable avant la constitution des rôles, à tous les détenteurs de logements potentiellement taxables selon les éléments en possession de l'administration, d'un courrier :
— rappelant les conditions d'assujettissement à la TLV,
— informant ses destinataires qu'ils sont susceptibles de recevoir prochaine ment un avis d'imposition à cette taxe, dès lors qu'ils ne sont pas soumis à la taxe d'habitation au titre de la vacance d'un logement depuis deux ans au 1er janvier dernier,
— les invitant à faire parvenir, s'il y a lieu, à leur centre des impôts, dans un délai précisé, les renseignements en leur possession qui les conduisent à esti mer qu'ils ne sont pas dans le champ d'application de la TLV,
— proposant des exemples de documents à produire auprès du centre des impôts de rattachement pour justifier du non-assujettissement à la taxe.

La Commission prend également acte de ce que :
— les éléments ainsi obtenus seront pris en compte lors de l'établissement des rôles, l'administration gardant bien évidemment la possibilité de contes ter les arguments présentés par la personne pour se soustraire à tout paie ment.
— ce courrier de demande de renseignements et d'information sur les don nées prises en compte pour l'assujettissement à la taxe annuelle sur les loge ments vacants sera adressé :

d'une part, aux personnes qui, ayant reçu, une année précédente, un avis d'imposition à la TLV et présenté une réclamation prise en compte par l'administration, ont bénéficié d'une mesure de dégrèvement et d'une suspension de l'imposition qui arrive à échéance,

. d'autre part, aux détenteurs de tout logement susceptible d'entrer pour la première fois dans le champ d'application de la loi au titre de sa vacance pendant la période de référence.

Les autres dispositions des demandes d'avis et des projets d'arrêtés qui leur sont joints n'appellent pas d'observations particulières.

En conséquence, après avoir pris acte, ainsi qu'il a été dit ci-dessus, des éléments nouveaux que la direction générale des Impôts a décidé d'adopter pour tenir pleinement compte de la nature et de la portée de la disposition applicable, la Commission :

Émet un avis favorable sur les quatre projets d'arrêtés qui lui sont soumis par le ministère de l'Économie, des finances et de l'industrie.

Délibération n° 00-044 du 3 octobre 2000 relative à la modification du traitement « ILIAD » de la direction générale des Impôts, et notamment à la mise en place du dossier « 2004 informatique ».

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 « modifiant l'arrêté du 25 juillet 1988 autorisant la création d'un traitement automatisé relatif à l'informatisation des inspections d'assiette et de documentation » (traitement « ILIAD »), 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 son article 11,

Vu le livre des procédures fiscales, notamment ses articles L. 45-O A, L. 169, L. 170 et R* 196-3,

Vu le décret n° 99-889 du 21 octobre 1999 transférant aux trésoriers-payeurs généraux le pouvoir de statuer sur les demandes d'admission en non-valeur présentées par les comptables du Trésor et supprimant la limitation de compétence des chefs de services déconcentrés des administrations financières pour statuer sur les demandes d'admission en non-valeur des créances fiscales irrécouvrables,

Après avoir entendu Monsieur Noël Chahid-Nouraï en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations,

Formule les observations suivantes :

L'application de la direction générale des Impôts (DGI) dénommée « ILIAD » a pour finalité d'assurer la gestion de l'impôt sur le revenu (IR), de la taxe d'habitation (TH), de la contribution sociale généralisée (CSG) et de la contribution au remboursement de la dette sociale (CRDS) ainsi que le traitement des affaires contentieuses concernant ces impôts. Elle est utilisée à titre principal, au sein des centres des impôts (CDI), par les agents des inspections d'assiette et de documentation.

Ce traitement a fait l'objet de plusieurs modifications, sur lesquelles la Commission est appelée à se prononcer :

— l'ajout d'une nouvelle finalité ayant trait à la mise en place du dossier « 2004 Informatique » dans le cadre du processus de dématérialisation de la documentation des CDI sur la fiscalité personnelle,

— l'organisation du transfert des dossiers magnétiques entre CDI en cas de déménagement des contribuables,

— la possibilité pour certains agents de la DGI et de la direction générale de la Comptabilité publique (DGCP) de disposer d'un accès direct à « ILIAD » en dehors des locaux du CDI gestionnaire de la base.

/. *Sur le contenu du dossier « 2004 Informatique »*

Le dossier « 2004 Informatique » réunit des informations de taxation relatives à l'année en cours, aux dernières années de taxation ainsi que des renseignements à validité permanente :

a) Au titre des données se rapportant à l'année en cours, le module « ILIAD IR/TH et Impositions supplémentaires » permet la consultation et la mise à jour des informations nécessaires à la taxation à l'IR, la TH, la CSG et la CRDS, notamment en cas d'établissement d'impositions supplémentaires. Les catégories d'informations traitées dans ce cadre concernent :

— les contribuables : l'état civil de la personne ou des conjoints, la raison sociale de la personne morale soumise à la TH, les adresses, le numéro FIP du foyer fiscal, la situation de famille, le nombre de personnes à charge, les revenus et charges pris en compte pour le calcul de l'assiette de l'IR, le relevé d'identité bancaire et la situation fiscale au regard de l'IR, de la TH et de la CSG/CRDS,

— les locaux entrant dans le champ de la TH : la localisation, la description, le type d'occupation, la valeur locative et la liste des occupants.

b) Au titre des informations à durée de vie pluri-annuelle, le « Résumé permanent » du dossier « 2004 Informatique » comporte les éléments d'état civil, la situation de famille et le numéro SPI des contribuables, le numéro FIP du foyer fiscal, les adresses dont l'ancienne adresse en cas de déménagement, le code des services successifs assurant la gestion du dossier, un code « dossier complexe » et divers renseignements sur la gestion interne du dossier.

c) Le « Résumé permanent » retrace également la situation des contribuables au regard de l'IR et de la CSG/CRDS pour chacune des dix dernières années de taxation, en conservant le revenu global imposable, les bases d'imposition CSG, le montant de ces impôts (primitif et rectifié) et les pénalités. De même, la clôture du dossier « 2004 Informatique » — en cas de décès, de disparition ou d'absence de dépôt d'une déclaration 2042 pendant plusieurs années successives —, ne conduit à l'effacement des informations qu'au terme d'un délai de dix ans à compter de la date de clôture.

La conservation pendant dix années de ces informations trouve son fondement dans l'article L. 170 du livre des procédures fiscales, qui autorise l'administration à réparer les omissions ou insuffisances d'imposition qui sont révélées par une instance devant les tribunaux ou par une réclamation contentieuse au plus tard jusqu'à la fin de la dixième année suivant celle au titre de laquelle l'imposition est due.

d) Des renseignements complémentaires sont, en outre, enregistrés pour cer taines années : le détail de la déclaration de revenus, de l'avis d'imposition ou de non imposition, de l'avis de restitution d'avoir fiscal et des documents de taxation initiaux et correctifs correspondants, les bulletins de recoupe ment issus des déclarations annuelles effectuées par les tiers payeurs, la na ture et le montant des déficits, la nature des engagements pris par le contribuable et le montant des déductions ou réductions d'impôt correspon dantes, ainsi que les avis d'imposition CSG/CRDS.

Ces éléments complémentaires sont normalement effacés au terme de la troi-sième année suivant l'année d'imposition, conformément au délai général de prescription. Ils sont toutefois conservés au-delà de ce délai aussi longtemps qu'ils remplissent l'une des conditions suivantes :

— ils permettent de contrôler des imputations de déficit ayant une validité au-delà du délai général de prescription,

— ils concernent des avis susceptibles d'être contestés par le contribuable pendant une durée spécifique (avis concernant une imposition supplémen taire ou une imposition initiale pénalisée),

— les impositions correspondantes font l'objet d'un recours contentieux en gagé par le contribuable,

— les annotations se rapportent à des engagements pris par les contribua bles qui peuvent avoir un effet sur les revenus des années non prescrites et dont il convient de s'assurer du respect.

Le détail des règles de conservation, qui sont applicables à certains des éléments du dossier « 2004 Informatique » par dérogation au délai général de prescription, étant spécifié chaque année dans une instruction interne de la DGI consacrée aux documents appelés normalement à être archivés, la Commission demande à en être rendue destinataire.

Le « Résumé permanent » est consultable à partir de l'état civil de la personne, de l'adresse ou du numéro FIP du foyer fiscal. En revanche, le numéro SPI ne constitue pas actuellement un critère d'interrogation de la base.

La Commission recommande, à cet égard, que le numéro SPI puisse, dans les meilleurs délais, servir de critère d'interrogation du traitement « ILIAD ».

e) Au sein du dossier « 2004 Informatique », un module dénommé « ILIAD Contentieux » a pour objet de permettre le suivi des réclamations, demandes gracieuses et demandes de renseignements adressées au CDI — à l'excep tion des demandes de droit d'accès présentées par les contribuables en ap plication de la loi du 6 janvier 1978. Il assure également la gestion des dégrèvements d'office et automatise le traitement des dégrèvements et des rappels IR, TH, CSG, CRDS en apportant une aide au calcul des répercus sions des dégrèvements et des rappels concernant l'IR sur les autres impôts et en facilitant leur transmission sur support magnétique aux services de la DGCP.

« ILIAD Contentieux » enregistre notamment :

— une analyse sommaire de la demande,

— les dates des différentes phases de la procédure administrative, à l'ex clusion de la phase juridictionnelle,
— une analyse sommaire de la décision administrative,
— une zone « bloc-notes » destinée à recevoir exclusivement des « infor mations directement liées à l'instruction des affaires contentieuses, à l'exclu sion de toute appréciation subjective, ainsi que les rectifications éventuellement apportées par le contribuable ou l'administration ». Ces in formations sont conservées pendant deux ans après la clôture de l'affaire.

La Commission appelle l'attention de la DGI sur les risques spécifiques qui sont associés à l'intégration dans un traitement automatisé d'une zone de commentaires libres, notamment du fait de la volatilité des informations qui y sont enregistrées, des difficultés à en contrôler la nature et la pertinence et des dérives qu'elle a pu constatées concrètement dans le cadre de contrôles portant sur d'autres assujettis à la loi du 6 janvier 1978. La Commission rappelle que, dans sa délibération n° 85-72 du 26 novembre 7 985, elle a demandé que la zone « bloc-notes » du traitement « RAR » de la DGCP, dont la finalité est la gestion des procédures contentieuses de recouvrement des impôts directs, fasse l'objet d'un droit d'accès immédiat, par la remise sans délai d'une copie d'écran effectuée à partir de l'imprimante du poste comptable.

En conséquence, la Commission insiste sur la nécessité d'attirer l'attention des utilisateurs du traitement sur les limitations apportées à l'utilisation de cette zone « bloc-notes ». Elle n'exclut pas, naturellement, que des contrôles spécifiques interviennent aux fins de vérifier si ces limitations sont respectées.

La Commission constate, par ailleurs, que le projet d'arrêté modificafif relatif à « ILIAD » n'apporte aucune précision sur les différentes règles retenues pour la définition de la durée de conservation, parfois longue, des informations enregistrées dans le dossier « 2004 Informatique ». C'est pourquoi elle demande qu'un nouvel article de l'arrêté énonce les règles relatives à la durée de conservation des informations dans « ILIAD ».

II. Sur le transfert des dossiers « 2004 INFORMATIQUE »

L'informatisation des dossiers fiscaux permet d'organiser leur transmission automatique entre CDI en cas de déménagement du contribuable. Après son transfert, le dossier peut encore être consulté pendant un an dans le CDI de départ, puis ne subsiste plus que sous la forme d'une fiche témoin informatique, où sont conservées les coordonnées des contribuables et du nouveau CDI gestionnaire du dossier.

Ce *dispositif, qui est de nature à faciliter les relations entre les contribuables et l'administration fiscale, n'appelle pas d'observation particulière.*

III. Sur la consultation de « ILIAD » en dehors des CDI ou par les agents des administrations financières autres que ceux des CDI

Dans le cadre du processus en cours de décloisonnement des administrations financières, il est proposé que l'ensemble des agents des services des impôts ait dorénavant vocation à procéder à des consultations ponctuelles des informations enregistrées dans l'application. Ils devront toutefois disposer d'une habilitation délivrée, sous sa responsabilité, par le responsable de centre gestionnaire de la base locale « ILIAD ».

S'agissant de la DGCP, les agents des trésoreries chargés des opérations de recouvrement et spécialement accrédités auprès du responsable du CDI ayant le même ressort territorial que la trésorerie peuvent avoir accès aux informations à partir des postes de travail implantés dans les locaux des CDI. Cet accès devrait les mettre en mesure d'éviter des erreurs d'homonymie et d'orienter les actions en recouvrement (choix des mesures de poursuites, octroi des échéanciers de paiement) en fonction de la situation personnelle, familiale et patrimoniale, du débiteur. De même, la connaissance d'une réclamation devrait permettre de demander la constitution de garanties en cas de demande de sursis de paiement, ou de s'abstenir de recourir à des poursuites lorsque les impositions émises paraissent ne pas être dues. Enfin, les bulletins de recoupement désignent indirectement certains tiers susceptibles d'être destinataires d'avis à tiers détenteur destinés à appréhender les sommes dont le redevable serait créancier.

La Commission rappelle que le projet d'arrêté n'a pas pour objet et ne saurait avoir pour effet d'étendre le droit de communication dont disposent les agents de la DGCP pour le recouvrement de certaines des catégories de créances dont ils sont chargés.

Elle demande, en outre, que le projet d'arrêté soit complété afin d'indiquer que les agents des administrations financières extérieurs au CDI gestionnaire des bases « ILIAD » peuvent consulter les informations, dans le cadre de leurs attributions, sous réserve de disposer d'une habilitation délivrée, sous sa responsabilité, par le responsable du centre gestionnaire.

La DGI souhaite, par ailleurs, que certains des destinataires susmentionnés puissent disposer d'un accès direct à « ILIAD », à partir de leurs locaux. ◦ cette fin, est prévue l'implantation de terminaux de consultation dans les locaux :

— des trésoreries paieries générales et des recettes des finances du réseau DGCP, au bénéfice des agents chargés de statuer sur les demandes d'admis sions en non-valeur, qui disposeront d'un accès à chacune des bases « ILIAD » des CDI correspondant à leur ressort territorial,

— des recettes des impôts du réseau DGI, dont les agents recourront à « ILIAD » à des fins de recouvrement de créances fiscales au même titre que les comptables du Trésor.

Un même accès direct pourrait bénéficier à l'ensemble des services des impôts comme à d'autres agents de la DGCP.

Sur ce dernier point, la Commission demande à être informée, le moment venu, de la liste des autres catégories de services susceptibles de bénéficier des mêmes modalités de consultation de « ILIAD », en précisant l'étendue des droits à consultation qu'il est envisagé de leur reconnaître ainsi que leur finalité.

S'agissant du dispositif de sécurité dont feront l'objet ces consultations externes, la Commission souhaite que la DGI apporte des précisions sur le détail des mesures prises pour assurer l'étanchéité du groupement fermé d'abonnés au sein duquel elles devraient s'effectuer.

Par ailleurs, la demande d'avis indique que la consultation de « ILIAD » par les agents des CDI peut s'effectuer à distance, dans des lieux excentrés, notamment dans le cadre d'une campagne d'information du public sur la déclaration de l'impôt sur le revenu.

La Commission rappelle, à cet égard, que la mise en place de procédures d'accès à distance doit être accompagnée d'un dispositif de sécurité prévoyant à la fois la reconnaissance physique du micro-ordinateur portatif utilisé et l'authentificafion de l'utilisateur.

Les autres dispositions de la demande d'avis modificative et du projet d'arrêté qui lui est joint n'appellent pas d'observations particulières.

Au bénéfice de ces observations, la Commission :

Émet un avis favorable sur le projet d'arrêté qui lui est soumis par le ministère de l'Economie, des Finances et de l'Industrie, **sous réserve :**

— que le projet d'arrêté modificatif soit complété en ce qui concerne les règles relatives à la durée de conservation des données dans l'application « ILIAD » et les conditions que doivent remplir les agents des administrations financières extérieurs au CDI gestionnaire de la base locale « ILIAD » pour pouvoir consulter l'application,

— que la Commission soit destinataire chaque année de l'instruction de la DGI prévoyant la conservation, au-delà du délai général de prescription, de certains des éléments du dossier « 2004 Informatique »,

— que la Commission soit tenue informée de la liste des nouvelles catégories d'agents et/ou de services susceptibles de consulter « ILIAD » à partir de leurs locaux, en précisant l'étendue des droits à consultation qu'il est envisagé de leur reconnaître ainsi que leur finalité, et qu'elle obtienne des précisions sur la nature des mesures prises pour assurer l'étanchéité du groupement fermé d'abonnés utilisé à cette occasion.

Délibération n° 00-046 du 12 octobre 2000 portant sur la demande d'avis présentée par l'INSEE relative à une enquête sur les déplacements et moyens de communication des ménages de la région stéphanoise.

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 portant création d'un traitement automatisé d'informations individuelles relatif à une enquête sur les déplacements et moyens de communication des ménages de la région stéphanoise ;

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, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Formule les observations suivantes :

La Commission est saisie, par la direction générale de l'INSEE, d'une demande d'avis concernant la mise en oeuvre d'un traitement automatisé d'informations nominatives à l'occasion d'une enquête sur les déplacements et moyens de communication des ménages de la région stéphanoise. Cette enquête, effectuée en partenariat avec le Syndicat intercommunal pour l'organisation des transports collectifs de l'agglomération stéphanoise (SIOTAS), a pour objectif de mieux cerner les pratiques de déplacement, l'utilisation des différents modes de transport, les opinions et les attitudes en matière de transport. Elle doit par ailleurs permettre de mesurer l'incidence de l'usage des nouvelles techniques de communication sur le volume des déplacements quotidiens des personnes.

La collecte, qui doit se dérouler entre octobre 2000 et janvier 2001, concerne 8 400 ménages répartis sur 68 communes du département de la Loire et 15 communes du département de la Haute-Loire.

L'enquête s'articule autour d'un questionnaire principal qui vise chaque membre du ménage âgé de 5 ans ou plus et d'un questionnaire d'opinion soumis à un seul membre du ménage âgé de 16 ans ou plus et tiré au sort.

Ces informations portent sur la composition du ménage, le logement du ménage et son équipement en matière de communication, les revenus annuels, la motorisation du ménage, le niveau d'étude atteint, les occupations et la profession exercées, l'adresse du lieu de travail, le lieu et le motif du déplacement, les raisons de l'utilisation ou non du réseau de transport en commun, l'intermodalité (ce chapitre ne concerne que les ménages ne se rendant pas à St-Etienne), le covoiturage (lorsque la personne choisie est active ou étudiante), les pratiques de déplacement pour les achats le samedi, la fréquentation vers les équipements (cinémas, théâtres, bibliothèques, équipements sportifs) et la desserte du logement.

Elles sont pertinentes au regard de la finalité poursuivie par l'enquête. La participation à l'enquête revêt un caractère facultatif, élément qui devrait être précisé à l'article premier de l'acte réglementaire. Les personnes concernées sont informées, conformément aux dispositions de l'article 27 de la loi du 6 janvier 1978, du caractère facultatif des réponses, des destinataires des données et de l'existence du droit d'accès.

L'INSEE est le seul destinataire des questionnaires et des fiches-adresses qui seront détruits dans les trois mois suivant la validation du fichier détail complet.

Le Syndicat intercommunal pour l'organisation des transports collectifs de l'agglomération stéphanoise (SIOTAS) et le Centre d'études techniques de l'équipement (CETE) sont seuls destinataires, après signature d'une convention avec l'INSEE, des fichiers de données anonymes relatifs aux ménages et aux personnes et comportant des zones géographiques inférieures à 2 000 habitants. Les données ainsi communiquées étant anonymes et agrégées à un niveau géographique fin, il conviendrait d'éviter l'ambiguïté que pourrait laisser substituer, à l'article 3 du projet d'acte réglementaire relatif aux destinataires, l'expression de « fichier de données individuelles anonymes » en supprimant le mot « individuelles ».

Au bénéfice de ces observations, la Commission :

Émet un **avis favorable** au projet d'arrêté portant création du traitement sous réserve de la précision à l'article premier qu'il s'agit d'une enquête facultative et de la suppression du terme « individuelles » à l'article 3.

Délibération n° 00-053 du 26 octobre 2000 concernant l'informatisation de la gestion par la direction générale des Impôts de la taxe annuelle sur les logements vacants.

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 « relatif à la mise en service par la direction générale des Impôts du traitement informatisé de la taxe annuelle sur les logements va cants » (traitement « TLV »),
— d'un projet d'arrêté « modifiant l'arrêté du 25 juillet 1988 autorisant la création d'un traitement automatisé relatif à l'informatisation des inspections d'assiette et de documentation » (traitement « ILIAD »),
— d'un projet d'arrêté « modifiant l'arrêté du 5 janvier 1990 relatif à la création d'un système automatisé de gestion de l'identité et des adresses des contribuables à l'impôt sur le revenu, à la taxe d'habitation et à l'impôt de solidarité sur la fortune » (traitement « FIP »),
— d'un projet d'arrêté « modifiant l'arrêté du 8 mars 1996 régissant le trai tement informatisé de la taxe d'habitation à la direction générale des Impôts » (traitement « TH »),

Saisie, en outre, d'une demande du commissaire du gouvernement relative à la portée de la délibération n° 00-043 du 3 octobre 2000 concernant les projets susmentionnés,

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 l'article 51 de la loi n° 98-657 du 29 juillet 1998 relative à la lutte contre les exclusions qui introduit un article 232 dans le code général des impôts, ensemble la décision n° 98-403 DC du 29 juillet 1999 du Conseil constitutionnel,

Vu la délibération n° 00-043 du 3 octobre 2000 de la Commission, concernant l'informatisation de la gestion par la direction générale des Impôts de la taxe annuelle sur les logements vacants,

Après avoir entendu Monsieur Noël Chahid-Nouraï en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations,

Formule les observations complémentaires suivantes :

Le traitement dénommé « TLV », qui fait l'objet de la première des demandes d'avis transmises par le ministère de l'Economie, des Finances et de l'Industrie à la Commission nationale de l'informatique et des libertés, a pour finalité d'assurer l'imposition des redevables de la taxe annuelle sur les logements vacants (TLV).

Dans sa précédente délibération, en date du 3 octobre 2000, la Commission a observé que la loi applicable définit l'assiette de la taxe (la valeur locative du logement), le taux d'imposition (qui varie selon la durée de la vacance), les personnes imposables (le propriétaire, l'usufruitier, le preneur à bail ou l'emphytéote), ainsi que les règles de contrôle, de recouvrement et de procédure contentieuse qui sont identiques à celles qui s'appliquent pour la taxe sur le foncier bâti.

La Commission a noté, en outre, que le Conseil constitutionnel, appelé à s'assurer de la constitutionnalité de cette disposition, a émis, dans sa décision du 29 juillet 1999, une réserve d'interprétation, ainsi énoncée : « l'objet de la taxation [étant] d'inciter les personnes [qui y sont assujetties] à mettre en location des logements susceptibles d'être loués [,] la différence de traitement fiscal instaurée par cet article entre [les bailleurs privés et publics et, parmi les bailleurs privés, entre les sociétés d'économie mixte de logement social et les autres propriétaires] n'est conforme à la Constitution que si les critères d'assujettissement [...] sont en rapport direct avec cet objet ; [...] ladite taxation ne peut dès lors frapper que des logements habitables, vacants et dont la vacance tient à la seule volonté de leur détenteur ».

La Commission a rappelé que, dans ces conditions, le Conseil constitutionnel a déclaré l'article 51 conforme à la Constitution, sous réserve d'une interprétation neutralisante, dont il résulte que « ne sauraient être assujettis » les « logements qui ne pourraient être rendus habitables qu'au prix de travaux importants et dont la charge incomberait nécessairement à leur détenteur », les « logements meublés affectés à l'habitation et, comme tels, assujettis [...] à la taxe d'habitation », les « logements dont la vacance est imputable à une cause étrangère à la volonté du bailleur, faisant obstacle à leur occupation durable, à titre onéreux ou gratuit, dans des conditions normales d'habitation, ou s'opposant à leur occupation, à titre onéreux ou gratuit, dans des conditions normales de rémunération du bailleur », les « logements ayant vocation, dans un délai proche, à disparaître ou à faire l'objet de travaux dans le cadre d'opérations d'urbanisme, de réhabilitation ou de démolition », ou les « logements mis en location ou en vente aux prix du marché et ne trouvant pas preneur ».

Et la Commission en a déduit qu'« *il résulte de ce qui précède d'une part que le champ d'exigibilité de la taxe sur les logements vacants n'inclut pas la totalité des logements inoccupés depuis au moins deux années consécutives au 1er janvier de l'année d'imposition, mais uniquement ceux qui, répondant à ce premier critère, n'entrent dans aucune des catégories susmentionnées, d'autre part et par voie de conséquence, que la taxation ne peut pas se déduire de la seule absence d'assujettissement à la taxe d'habitation ».*

Or — ainsi que la Commission l'a constaté dans ses précédentes délibérations — il est prévu, en ce qui concerne le recensement des personnes assujetties à la taxe, d'utiliser, dans un premier temps, les informations gérées par le traitement « TH » afin d'obtenir la liste des logements identifiés

comme étant vacants au sens de la taxe d'habitation alors que cette première sélection ne permet pas d'exclure certaines catégories de logements qui n'entrent pas dans le champ d'application de la TLV, tels que les logements qui ne sont pas habitables (non clos), ceux qui ont été occupés temporairement plus de 30 jours au cours de l'une des deux précédentes années, ceux dont la vacance trouve son origine dans la nécessité de réaliser d'importants travaux, ceux qui doivent être prochainement détruits ou encore ceux qui ne trouvent pas preneur, bien qu'étant mis en vente ou en location au prix du marché.

C'est pourquoi la DGI prévoit de mettre ces informations à la disposition des CDI, via le traitement « ILIAD », préalablement à toute taxation, afin que ces services — les mieux à même d'apprécier les situations concrètes — aient la possibilité de s'opposer, sur la base des justificatifs déjà adressés par les intéressés ou de leur connaissance du terrain, à l'assujettissement des logements au cas par cas. Les CDI ont la faculté de modifier deux informations au sein du fichier « ILIAD », en vue de leur communication au traitement « TLV » :

— l'indication de la vacance du logement au sens de la taxe d'habitation,

— l'année à partir de laquelle sera décomptée la période de référence de la taxe, qui servira pour déterminer l'année où le logement sera potentielle ment imposable.

Cependant, dès lors que les CDI ne disposent pas, au titre de la gestion d'une autre imposition, de l'ensemble des éléments factuels pertinents pour identifier les personnes qui entrent dans le champ d'application de la TLV, seule la collecte, dès avant l'émission des rôles de la TLV et l'envoi des avis d'imposition, d'informations complémentaires auprès des personnes susceptibles d'être concernées au vu des listes transmises par l'application « TH » est de nature à éviter d'imposer à la taxe des contribuables qui ne répondraient pas aux critères de taxation posés par la loi.

Dans ces conditions, la Commission avait initialement entendu formuler des réserves concernant l'envoi par la DGI *dans un délai raisonnable avant la constitution des rôles, à tous les détenteurs de logements potentiellement taxables selon les éléments en possession de l'administration, d'un courrier :*

— *rappelant les conditions d'assujettissement à la TLV,*

— *informant ses destinataires qu'ils sont susceptibles de recevoir prochaine ment un avis d'imposition à cette taxe, dès lors qu'ils ne sont pas soumis à la taxe d'habitation au titre de la vacance d'un logement depuis deux ans au 1er janvier dernier,*

— *les invitant à faire parvenir, s'il y a lieu, à leur centre des impôts, dans un délai précisé, les renseignements en leur possession qui les conduisent à esti mer qu'ils ne sont pas dans le champ d'application de la TLV,*

— *proposant des exemples de documents à produire auprès du centre des impôts de rattachement pour justifier du non-assujettissement à la taxe ;*

Selon la Commission :

— *les éléments ainsi obtenus devaient être pris en compte lors de l'établisse ment des rôles, l'administration gardant bien évidemment la possibilité de contester les arguments présentés par la personne pour se soustraire à tout paiement ;*

— *le courrier sus-évoqué de demande de renseignements et d'information sur les données prises en compte pour l'assujettissement à la taxe annuelle* sur /es *logements vacants devait être adressé :*

. d'une part, aux personnes qui, ayant reçu, une année précédente, un avis d'imposition à la TLV et présenté une réclamation prise en compte par l'administration, ont bénéficié d'une mesure de dégrèvement et d'une suspension de l'imposition qui arrive à échéance,
. d'autre part, aux détenteurs de tout logement susceptible d'entrer pour la première fois dans le champ d'application de la loi au titre de sa vacance pendant la période de référence.

Ayant compris, sur la base des indications qui lui avaient été fournies en séance, que la DGI acceptait les réserves qui devaient être ainsi formulées, la Commission, dans sa délibération susvisée, a pris acte de ce que le courrier sus-évoqué serait envoyé par les services compétents et qu'il serait tenu compte des réponses apportées par les contribuables lors de l'établissement des rôles.

La Commission constate, compte tenu des indications additionnelles qui lui sont fournies par le commissaire du gouvernement, que l'acquiescement de la DGI ne se trouve pas en réalité acquis au principe de la mesure, les Services considérant cependant que, lorsqu'une réserve se trouve émise par la CNIL, il leur incombe d'y déférer.

En conséquence, après avoir pris acte, ainsi qu'il a été dit ci-dessus, des éléments nouveaux que le commissaire du gouvernement a communiqués, la Commission :

Emet un **avis favorable** sur les quatre projets d'arrêtés qui lui ont été soumis par le ministère de l'Économie, des Finances et de l'Industrie **sous les réserves suivantes :**

1) la DGI adressera dans un délai raisonnable avant la constitution des rô les, à tous les détenteurs de logements potentiellement taxables selon les élé ments en possession de l'administration, un courrier :
— rappelant les conditions d'assujettissement à la TLV,
— informant ses destinataires qu'ils sont susceptibles de recevoir prochaine ment un avis d'imposition à cette taxe, dès lors qu'ils ne sont pas soumis à la taxe d'habitation au titre de la vacance d'un logement depuis deux ans au 1er janvier dernier,
— les invitant à faire parvenir, s'il y a lieu, à leur centre des impôts, dans un délai précisé, les renseignements en leur possession qui les conduisent à esti mer qu'ils ne sont pas dans le champ d'application de la TLV,
— proposant des exemples de documents à produire auprès du centre des impôts de rattachement pour justifier du non-assujettissement à la taxe ;

2) Le courrier sus-évoqué de demande de renseignements et d'information sur les données prises en compte pour l'assujettissement à la taxe annuelle sur les logements vacants devra être adressé :
— d'une part, aux personnes qui, ayant reçu, une année précédente, un avis d'imposition à la TLV et présenté une réclamation prise en compte par l'administration, ont bénéficié d'une mesure de dégrèvement et d'une sus pension de l'imposition qui arrive à échéance,
— d'autre part, aux détenteurs de tout logement susceptible d'entrer pour la première fois dans le champ d'application de la loi au titre de sa vacance pendant la période de référence.

3) Les éléments obtenus grâce aux réponses des contribuables seront pris en compte lors de l'établissement des rôles étant entendu que l'administration

fiscale gardera la possibilité de contester les arguments éventuellement présentés par la personne pour se soustraire à tout paiement.

Délibération n° 00-055 du 16 novembre 2000 portant sur la demande d'avis présentée par l'INSEE relative à la mise en oeuvre d'une enquête dénommée « Sans domicile 2001 »

La Commission nationale de l'informatique et des libertés, Saisie pour avis par le ministre de l'Economie, des Finances et de l'Industrie d'un projet d'arrêté portant création d'un traitement automatisé d'informations individuelles relatif à une enquête auprès des personnes fréquentant les lieux d'hébergement ou de restauration gratuits ;

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, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Formule les observations suivantes :

La Commission est saisie, par la direction générale de l'INSEE, d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé d'informations nominatives à l'occasion d'une enquête menée auprès de 4 000 personnes fréquentant les lieux d'hébergement ou de restauration gratuits. Cette enquête facultative a pour objectif de décrire les conditions de vie et les difficultés d'accès au logement des personnes sans domicile, ce qui n'a, à ce jour, jamais été réalisé au niveau national.

La collecte des données, qui doit se dérouler en janvier — février 2001, concerne 4 000 personnes de 18 ans et plus qui, dans les agglomérations de plus de 20 000 habitants, fréquentent au moins une fois pendant la période de l'enquête un service d'hébergement ou de restauration gratuite. Les personnes interrogées sont contactées par l'intermédiaire des services fréquentés ; cette médiation est justifiée par le caractère novateur de l'enquête qui s'adresse à une population ne disposant pas de logement et qui, dès lors, échappe aux enquêtes traditionnellement effectuées par l'INSEE auprès des ménages.

Les informations collectées portent sur les caractéristiques socio-démographiques du répondant, la situation vis-à-vis du logement, la situation vis-à-vis du marché du travail, les conditions d'emploi, la rémunération, les difficultés

financières et l'endettement, les prestations et aides reçues, les raisons de non recours à certaines aides, la santé et l'accès aux soins, les conditions de vie dans les lieux et les structures d'accueil, des éléments simples de biographie.

La rubrique relative aux caractéristiques socio-démographiques prévoit le recueil de la date de naissance de la personne interrogée. Il convient, afin de renforcer l'anonymat, de substituer à la date de naissance, le mois de naissance.

Ces informations sont pertinentes au regard de la finalité poursuivie par l'enquête.

La participation à l'enquête est facultative ; les personnes concernées sont informées, conformément aux dispositions de l'article 27 de la loi du 6 janvier 1978, du caractère facultatif des réponses, des destinataires des données et de l'existence du droit d'accès.

L'INSEE est le seul destinataire des questionnaires et des fiches adresses qui seront détruits dans les trois mois suivant la validation du fichier détail complet.

Au bénéfice de ces observations, la Commission :

Émet un **avis favorable** au projet d'arrêté portant création du traitement, sous réserve de la modification de la rubrique A3 du questionnaire afin que ne soit collectée que l'année de naissance.

Délibération n° 00-058 du 16 novembre 2000 portant avis sur un projet de décret présenté par le secrétariat d'État à l'Outre-mer relatif à la création d'un traitement automatisé nécessaire à la tenue du fichier général des électeurs inscrits à Mayotte.

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le secrétariat d'Etat à l'Outre-mer d'un projet de décret visant à créer un traitement informatisé constituant le fichier général des électeurs inscrits sur les listes électorales de Mayotte ;

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, notamment son article 5 ;

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

Vu les ordonnances n° 98-730 du 20 août 1998 et n° 2000-350 du 19 avril 2000 portant actualisation et adaptation du droit électoral applicable outre-mer ;

Vu le projet de décret présenté par le Secrétaire d'Etat à l'Outre-mer ;

Après avoir entendu Monsieur Maurice Benassayag en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

L'article 3-11 de l'ordonnance n° 2000-350 du 19 avril 2000 confie la tenue du fichier général des électeurs au représentant du gouvernement. Ce fichier est tenu, en métropole, par l'Institut national de la statistique et des études économiques (INSEE).

Le fichier général des électeurs de Mayotte comprend les listes électorales dites « générales » et les listes électorales dites « complémentaires » pour, d'une part, l'élection au Parlement européen et, d'autre part, l'élection des conseils municipaux.

Il est mis à jour à partir des décisions d'inscription ou de radiation des commissions administratives chargées de réviser les listes électorales, des décisions judiciaires relatives à l'inscription ou à la radiation d'un électeur, des avis de perte ou de recouvrement de capacité électorale transmis par le casier judiciaire, des avis de décès établis par les mairies, ainsi que des avis reçus de l'INSEE ou des représentants de l'État chargés du contrôle des listes électorales demandant la radiation d'un électeur des listes de Mayotte, ou informant du décès d'un électeur ou encore faisant part d'une décision privative des droits civils et politiques hors de la Mayotte.

Les catégories d'informations traitées sont relatives à l'identité de l'électeur, à la date et au lieu de la demande d'inscription, à la date de l'inscription, au type de liste électorale, à la perte des droits civils et politiques (date d'effet et durée), à l'acquisition ou à la perte de la nationalité française, au décès et à la nationalité pour les ressortissants de l'Union européenne.

Les destinataires des informations traitées sont l'INSEE, l'Institut territorial de la statistique et des études économiques en Nouvelle-Calédonie et, en Polynésie française et dans les îles de Wallis et Futuna, le représentant de l'Etat chargé du contrôle des listes électorales, ainsi que les maires pour ce qui concerne leur commune, aux fins de contrôle d'éventuelles doubles inscriptions et de mise à jour des listes électorales.

Le droit d'accès des personnes concernées s'exercera, en application de l'article 34 de la loi du 6 janvier 1978, auprès du représentant du gouvernement à Mayotte. Compte tenu de ces observations, la Commission :

Émet un **avis favorable** au projet de décret présenté par le secrétaire d'État à l'Outre-mer.

Délibération n° 00-059 du 30 novembre 2000 portant avis sur un projet d'arrêté modifiant l'arrêté du 28 avril 1993 présenté par le ministère de la Justice relatif à un traitement national ayant pour finalité le suivi des mesures éducatives et de l'activité des services du secteur public de la protection judiciaire de la jeunesse.

La Commission nationale de l'informatique et des libertés, Saisie par le ministre de la Justice d'un projet d'arrêté modifiant l'arrêté du 28 avril 1993 organisant le traitement automatisé des statistiques des établissements et services de l'administration de la protection judiciaire de la jeunesse dénommé « GAME »,

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 avril 1993 organisant le traitement automatisé des statistiques des établissements et services de l'administration de la protection judiciaire de la jeunesse ;

Vu la délibération de la CNIL n° 93-022 du 9 mars 1993 ;

Vu le projet d'arrêté présenté par le Garde des Sceaux, ministre de la Justice ;

Après avoir entendu Monsieur Gérard Gouzes, vice-président, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

Les juridictions de la jeunesse confient l'exécution d'une partie des mesures éducatives qu'elles ordonnent aux établissements et services publics de la protection judiciaire de la jeunesse. Ces services ont l'obligation de suivre le déroulement de l'accomplissement des mesures qui leur sont confiées et d'en rendre compte, tant au magistrat mandant qu'aux échelons supérieurs de la hiérarchie administrative (établissement et services, direction départementale, direction régionale et administration centrale).

Le traitement GAME a une double finalité consistant, d'une part, à assurer la gestion d'un fichier nominatif des mesures effectuées à l'échelon local (dans les établissements et services de protection judiciaire de la jeunesse) et départemental (dans les directions départementales de protection judiciaire de la jeunesse) et, d'autre part, à permettre la constitution, au niveau des directions régionales de protection judiciaire de la jeunesse et de la direction centrale, de fichiers à des fins statistiques en vue de connaître la population des jeunes bénéficiant de mesures de protection judiciaire.

Le projet d'arrêté modificatif dont est saisie la Commission a pour objet, d'une part, d'assurer un meilleur suivi au plan local des mesures éducatives par l'ajout de nouvelles informations et, d'autre part, de permettre la remontée d'informations anonymisées plus complètes au niveau régional et national.

La première modification envisagée porte sur l'ajout, au sein des fichiers nominatifs détenus par les établissements et services et les directions départementales de la protection judiciaire de la jeunesse, des catégories d'informations suivantes : le sexe du jeune, la profession, l'adresse et l'âge des parents et/ou du tuteur, le nombre d'enfants dans la fratrie et le point de savoir s'ils sont connus des services de protection judiciaire de la jeunesse, ainsi que la situation scolaire du jeune.

Le recueil de ces informations complémentaires, dans la mesure où elles sont destinées à permettre un meilleur suivi des jeunes par les établissements et

par l'échelon départemental est pertinent, adéquat et non excessif au regard de la finalité du traitement.

La deuxième modification envisagée vise à permettre la transmission d'informations complémentaires aux directions régionales et à la direction centrale de la protection judiciaire de la jeunesse. Ces informations complémentaires seraient les suivantes : le nom au jeune, sous une forme cryptée, ses sexe, date de naissance, département et pays de naissance, code postal et quartier de résidence, le nombre d'enfants de la fratrie, la situation maritale des père et mère et/ou du tuteur, la qualité du titulaire de l'autorité parentale (à l'exclusion de son identité) ainsi que la date de création de la fiche et le code de l'établissement concerné.

La transmission de ces informations doit permettre à l'administration de la protection judiciaire de la jeunesse de disposer d'une description plus précise des caractéristiques de la population prise en charge afin, notamment, de mieux adapter les structures d'accueil et les mesures à prendre. ◦ cette fin, les directions régionales et la direction centrale de la protection judiciaire de la jeunesse n'ont pas à connaître l'identité des jeunes, des informations anonymisées étant suffisantes.

Il importe à cet effet que l'identité des jeunes fasse l'objet d'une procédure de chiffrement irréversible. **Prend acte** de ce que : La direction de la protection judiciaire de la jeunesse s'est engagée à :

— rendre techniquement impossible, dans les fichiers des établissements, services et des directions départementales, tout recoupement entre l'identi fiant crypté du jeune et son identité en clair ;

— à saisir la Direction centrale de la sécurité des systèmes d'informations (DCSSI) afin que celle-ci puisse évaluer la qualité du dispositif de cryptage retenu et son niveau de sécurité ;

Émet, en conséquence, **un avis favorable** au projet d'arrêté modificafif soumis par le Garde des Sceaux, ministre de la Justice.

Annexe 6

Décisions des juridictions

ARRêT DU CONSEIL D'ÉTAT DU 30 JUIN 2000

Affaire Ligue française pour la défense des droits de l'homme et du citoyen

(Req. n° 210412)

Vu la requête sommaire et le mémoire complémentaire, présentés pour la Ligue française pour la défense des droits de l'homme et du citoyen demandant l'annulation pour excès de pouvoir du décret n° 99-362 du 6 mai 1999 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies visées à l'article L. 11 du code de la santé publique et modifiant le code de la santé publique (deuxième partie : Décrets en Conseil d'État) ;

Sur la légalité externe du décret attaqué :

Sur le moyen tiré du défaut de consultation de la Commission nationale de l'informatique et des libertés :

Considérant, en premier lieu, que 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, invoquée par l'association requérante, définit, dans son article 2, un « traitement de données à caractère personnel » comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte [...], la communication par transmission » ; qu'il résulte clairement de cette définition que la collecte des données individuelles concernant les cas de maladies visées à l'article L. 11 du code de la santé publique, en vue de leur transmission à l'autorité sanitaire, constitue un traitement de données à caractère personnel au sens de la directive ;

Considérant, en deuxième lieu, qu'aux termes de l'article 20 de la même directive, qui déroge au principe général énoncé à l'article 18 selon lequel les traitements compris dans le champ de la directive ne font l'objet que d'une notification à l'autorité de contrôle établie, en application de l'article 28, dans chaque État membre pour surveiller sur son territoire l'application du dispositif national de protection : « 1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre. / 2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement [...] ; / 3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées », qu'il résulte clairement de ces dispositions que le choix est laissé aux États membres de faire procéder à l'examen préalable des traitements qu'ils identifient comme présentant des risques particuliers soit à la suite de leur notification à l'autorité de contrôle, soit, plutôt, lors de l'élaboration de la loi ou du règlement d'application qui définit la nature du traitement ainsi que les droits et garanties qui y sont attachés ;

Considérant que, dans l'attente de la transposition de la directive 95/46/CE dans le droit national, les traitements devant faire l'objet d'un examen préalable au sens de l'article 20 de la directive sont ceux compris dans le champ de l'article 15 de la loi du 6 janvier 1978, dont la création est décidée par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des

libertés, qui doit être regardée comme l'autorité de contrôle française pour l'exercice des missions prévues par l'article 28 de la directive ; que si la Commission nationale de l'informatique et des libertés devait ainsi être consultée préalablement à la mise en œuvre du traitement ou du groupe de traitements dont la nature ainsi que certaines garanties qui y sont attachées sont définies par le décret du 6 mai 1999 pris pour l'application de l'article L. 11 du code de la santé publique, le gouvernement, en s'abstenant de faire procéder à cet examen lors de l'élaboration de ce décret et en prévoyant, par un renvoi à l'article 15 de la loi du 6 janvier 1978, que la consultation de la Commission nationale de l'informatique et des libertés aurait lieu à l'occasion de la transmission ultérieure à cette commission des projets d'arrêtés du ministre chargé de la santé créant les traitements, accompagnés de l'ensemble des informations et précisions exigées par les articles 19 et 20 de la loi du 6 janvier 1978, n'a fait qu'exercer le choix autorisé par l'article 20 de la directive dont il n'a pas, par conséquent, méconnu les objectifs ;

Considérant, en troisième lieu, que si l'association requérante invoque les dispositions du paragraphe 2 de l'article 28 de la directive selon lesquelles « chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel », il résulte clairement de ces dispositions que la seule obligation qu'elles instituent est de soumettre à la consultation préalable de l'autorité de contrôle les projets de textes qui, sans avoir pour objet la création d'un traitement ou d'un groupe de traitements, définissent le cadre général de la protection des droits et libertés des personnes à l'égard du principe du traitement de données à caractère personnel ; que tel n'est pas l'objet du décret attaqué qui, ainsi qu'il vient d'être dit ci-dessus, relève exclusivement de la procédure prévue à l'article 20 de la directive ;

Considérant qu'il résulte de tout ce qui précède que le moyen tiré de ce que le décret aurait dû être précédé de la consultation de la Commission nationale de l'informatique et des libertés doit être écarté ;

Sur l'autre moyen de légalité externe :

Considérant qu'il ressort des pièces du dossier, et notamment de l'avis du Conseil d'État en date du 2 février 1999 dont le texte a été communiqué par le ministre de l'Emploi et de la Solidarité en annexe à son mémoire en défense, que le texte du décret attaqué ne diffère pas de celui adopté par le Conseil d'Etat ; que, dès lors, le moyen tiré de ce que le texte du décret attaqué ne serait pas conforme à la version transmise par le gouvernement au Conseil d'Etat ou à celle adoptée par le Conseil d'Etat doit être écarté ;

Sur la légalité interne du décret attaqué : En

ce qui concerne l'article R. 11-2 :

Considérant qu'aux termes de l'article L. 11 du code de la santé publique dans sa rédaction issue de la loi du 1er juillet 1998 relative au renforcement de la veille sanitaire et du contrôle de la sécurité sanitaire de produits destinés à l'homme : « Font l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire par les médecins et les responsables des services et laboratoires d'analyse de biologie médicale publics et privés : 1° Les maladies qui nécessitent une intervention urgente locale, nationale ou internationale ; 2° Les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique. Un décret pris après avis du Conseil supérieur d'hygiène publique de France définit la liste des maladies correspondant aux 1° et 2°. Les modalités de la transmission des données à

l'autorité sanitaire dans les deux cas, en particulier la manière dont l'anonymat est protégé, sont fixées par décret en Conseil d'État »,

Considérant que si l'article R. 11 -2 inséré dans le code de la santé publique par le décret du 6 mai 1999 pris pour l'application des dispositions législatives précitées prévoit que la transmission des données individuelles concernant les cas de maladies figurant sur la liste mentionnée à l'article L. 11 du même code doit demeurer confidentielle, et, à cette fin, définit de manière limitative les autorités sanitaires qui en sont les destinataires et prévoit que la notification à ces dernières a lieu « sous pli confidentiel ou après chiffrement des données », il se borne, en ce qui concerne la nature des informations pouvant figurer sur la fiche individuelle établie pour maladie, à renvoyer à un arrêté du ministre chargé de la santé la fixation « des éléments à caractère nominatif » portés sur la fiche, « sous réserve de l'application des dispositions de l'article 15 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » ;

Considérant que s'il appartenait éventuellement au gouvernement, après avoir défini avec une précision suffisante dans le décret en Conseil d'Etat les principes qu'il entendait retenir pour protéger, comme le lui demandait le législateur, l'anonymat des personnes dont les données individuelles sont ainsi recueillies, de renvoyer à un arrêté ultérieur le soin de préciser, en tenant compte éventuellement de la nature de la maladie ou de l'objectif poursuivi par la collecte, les modalités de l'application de ces principes, il ne pouvait se décharger légalement de la mission que lui avait confiée l'article L. 11 précité en se bornant à renvoyer purement et simplement à un arrêté ministériel le soin de déterminer les règles concernant l'objet ci-dessus défini ; qu'il suit de là que le premier alinéa de l'article R. 11 -2 est entaché d'excès de pouvoir ;

En ce qui concerne l'article R. 11-3 :

Considérant que l'article R. 11-3 inséré au code de la santé publique impose aux professionnels de santé ayant constaté l'existence d'un cas de maladie nécessitant, au sens du 1 ° de l'article L. 11 du code de la santé publique, une intervention urgente locale, nationale ou internationale, l'obligation non seulement de notifier les données individuelles en application de l'article R. 11-2, mais également de « signaler sans délai » le cas constaté, afin de « permettre la mise en place d'urgence de mesures de prévention individuelle et collective et, le cas échéant, de déclencher des investigations pour identifier l'origine de la contamination ou de l'exposition » ; en prévoyant, aux quatrième et cinquième alinéas de l'article R. 11-3, d'une part, « qu'à la demande du médecin destinataire du signalement le déclarant est tenu de lui fournir toute information nécessaire à la mise en œuvre des mesures d'investigation et d'intervention, y compris l'identité et l'adresse du patient », d'autre part, « que ces informations peuvent être transmises à d'autres professionnels lorsque leur intervention est indispensable pour la mise en œuvre des mesures de prévention individuelle et collective », le gouvernement n'a pas excédé les limites de l'habilitation reçue du législateur qui l'invitait au contraire, pour les maladies figurant au 1 ° de l'article L 11, à concilier le principe de l'anonymat avec la nécessité de protéger la santé publique dans les cas où celle-ci requiert une intervention urgente ; que la règle qu'il a édictée, en la complétant au même article R. 11-3 de la précaution selon laquelle les informations ainsi communiquées ne sont conservées que « le temps nécessaire à l'intervention ou à l'investigation », est proportionnée à l'objectif poursuivi ; que le moyen tiré de la violation de l'article L 11 au code de la santé publique doit, par suite, être écarté ;

Décide :

Art. 1er : Le premier alinéa de l'article R. 11-2 inséré dans le code de la santé publique par le décret n° 99-362 du 6 mai 1999 est annulé.

Art. 2 : Le surplus des conclusions de la requête est rejeté.

ARRتT DU CONSEIL D'ÉTAT DU 28 JUILLET 2000

Affaire Mme T. (Req. n° 210311)

Sur la compétence du Conseil d'Etat :

Considérant qu'aux termes de l'article 2 du décret susvisé du 30 septembre 1953 : « Le Conseil d'État reste compétent pour connaître en premier et dernier ressort : [...] 6e des recours en annulation dirigés contre les décisions administratives des organismes collégiaux à compétence nationale » ; que Mme T. demande au Conseil d'Etat d'annuler la décision en date du 15 juin 1999 par laquelle le président de la Commission nationale de l'informatique et des libertés a clos le dossier relatif à sa demande de vérification portant sur la finalité et l'usage d'un fichier nominatif de l'association des anciens élèves du Centre d'études littéraires et scientifiques appliquées (CELSA) ;

Considérant qu'aux termes du deuxième alinéa de l'article 10 de la loi du 6 janvier 1978 susvisée : « La commission peut charger le président [...] d'exercer ses attributions en ce qui concerne l'application des articles 16, 17, 21 (4°, 5° et 6°) » ; qu'aux termes de l'article 21 : « Pour l'exercice de sa mission de contrôle, la commission : [...] 6° reçoit les réclamations, pétitions, plaintes » ; que par sa délibération du 3 février 1999 la Commission nationale de l'informatique et des libertés a chargé son président d'exercer en son nom les attributions concernant l'application des articles 16, 17 et 21 (4°, 5° et 6°) de la loi du 6 janvier 1978 susvisée ; que le président de la Commission nationale de l'informatique et des libertés, en prenant la décision attaquée, n'a pas agi en vertu de ses pouvoirs propres, mais dans l'exercice des attributions de la commission ; que, par suite, le Conseil d'État est compétent pour connaître en premier et dernier ressort de la demande de Mme T. ;

Sur la légalité de la décision attaquée :

Considérant que le moyen tiré par Mme T. de ce que la vérification opérée par la Commission nationale de l'informatique et des libertés aurait été insuffisante n'est pas assorti de précision permettant d'en apprécier la portée ;

Considérant que le moyen tiré de ce que la Commission nationale de l'informatique et des libertés n'aurait pas dû communiquer à l'association le nom de la personne l'ayant saisie pour vérification est sans incidence sur la légalité de la décision attaquée ;

Considérant qu'il résulte de ce qui précède que Mme T. n'est pas fondée à demander l'annulation de la décision qu'elle attaque ;

Décide :

Art. - 1er : La requête de Mme T,. est rejetée.

Annexe 7

Actualité parlementaire

CNIL

Moyens financiers

8954 — 19 janvier 1998. **M. Guy Drut** attire l'attention de **M. le ministre de l'Intérieur** sur la nécessité de donner des moyens matériels supplémentaires à la Commission nationale de l'informatique et des libertés. En effet, il semble difficile à cet organisme de gérer de plus en plus de demandes d'autorisations avec des moyens humains et matériels qui n'évoluent pas en proportion. Il lui demande donc quelles mesures il compte prendre pour faciliter l'action de la CNIL qui a reçu, en 1996, plus de 3 500 demandes d'autorisations de constitution de fichiers. ***Question transmise à M. le Premier ministre.***

Réponse. — Dans le cadre du budget 2001, les moyens de la Commission nationale de l'informatique et des libertés ont progressé de façon significative (+ 18,35 %), pour tenir compte de l'accroissement de son activité (budget 2000 : 32,5 MF ; budget 2001 : 38,5 MF). En 2001, la Commission bénéficiera de 12 emplois supplémentaires. Ainsi, ses effectifs passeront de 58 agents en 2000 à 70 en 2001. S'agissant des dépenses de fonctionnement, les crédits progressent de 2,593 MF, soit une augmentation de 24,57 *%.* Enfin, compte tenu des moyens supplémentaires en personnels qui lui sont alloués et du développement de son activité, il est envisagé de regrouper l'ensemble des services de la CNIL sur un seul site (au lieu de deux actuellement), ce qui rendra plus efficace son fonctionnement.

Assemblée nationale, 11 décembre 2000, n° 50 (p. 6970)

Dénonciation au parquet

27051 — 27 juillet 2000. — **M. Serge Mathieu** demande à **M^me^ le Garde des Sceaux, ministre de la Justice,** de lui préciser les réflexions que lui inspire la prise de position justifiée de la Commission nationale informatique et libertés (CNIL) dénonçant, au parquet de Paris, l'Eglise de Scientologie d'Ile-de-France, à l'égard de la tenue de ses fichiers *{Le Monde* du 28 juin 2000).

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'en application de l'article 21 alinéa 4 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés « adresse aux intéressés des avertissements et dénonce au Parquet les infractions dont elle a connaissance conformément à l'article 40 du code de procédure pénale ». C'est à ce titre que cette commission a, le 21 juin 2000, saisi le procureur de la République près le tribunal de grande instance de Paris du dossier évoqué dans la question. Les faits dénoncés étant connexes à ceux instruits dans le cadre d'une information judiciaire suivie au tribunal de grande instance de Paris, le juge d'instruction a été supplétivement saisi.

Sénat, 23 novembre 2000, n° 46 (p. 4021)

INTERNET

Régulation

33750 — 9 août 1999. — **M. Olivier de Chazeaux** appelle l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur la protection des données sur Internet. Il l'interroge notamment sur la transposition de la directive relative

à la protection des données personnelles. En effet, alors que l'Europe et les États-Unis conduisent des discussions sur ce thème visant à la publication de matériaux portant sur les moyens de garantir des « bases sécurisées » *(safe harbour),* la France semble tirer argument de son avance dans la matière pour ne pas procéder à la transposition de la directive. C est pourquoi il lui demande de faire le point sur ces questions.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la directive n° 95/46/CE du Parlement européen et du conseil 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 devait être transposée en droit national dans un délai de trois ans après son adoption. Ce texte communautaire, dans la mesure notamment où il conduit les États membres de l'Union européenne à prendre des dispositions protectrices en matière d'échanges transfrontières de données avec des pays tiers à celle-ci, a des incidences importantes quant à l'encadrement d'Internet. Il implique du reste sur d'autres points des modifications substantielles de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En tout état de cause, la France ne saurait tirer argument de ce qu'elle s'est dotée, il y a plus de vingt ans, d'une législation pionnière en matière de protection des données pour éluder ses obligations communautaires. Le retard pris par cette transposition s'explique, outre par le changement de gouvernement intervenu au printemps 1997, par la nécessité d'adapter le régime actuel aux bouleversements considérables qui ont affecté depuis 1978 la place tenue par l'informatique dans la société contemporaine, en tenant compte de la circulation accrue que connaissent aujourd'hui les données à caractère personnel et de l'exigence de préserver un niveau élevé de protection des droits fondamentaux des personnes. Ces exigences ont rendu indispensables, en préalable à la préparation d'un texte, une réflexion et des travaux préparatoires de grande ampleur, parmi lesquels il convient de souligner l'importance du rapport intitulé « Données personnelles et société de l'information », remis au Premier ministre par M. Guy Braibant en mars 1998, ainsi que celle de l'étude du Conseil d'État sur Internet et les réseaux numériques, rendue publique à l'automne 1998. C'est en s'appuyant sur ces différents travaux que la Chancellerie a élaboré, début 1999, un avant-projet de loi de transposition, dont l'examen interministériel a eu lieu au second semestre 1999, et qui doit encore être soumis, pour avis, conformément aux dispositions en vigueur pour des projets qui touchent à la protection des libertés individuelles, à la Commission nationale informatique et des libertés (CNIL) et à la Commission nationale consultative des droits de l'homme (CNCDH). Le projet de loi, éventuellement complété afin de tenir compte des avis de ces deux autorités administratives indépendantes, sera alors soumis au Conseil d'Etat, puis examiné en Conseil des ministres dans quelques semaines. Ainsi, le Parlement pourra-t-il être saisi à bref délai de ce texte auquel le gouvernement attache une très grande importance et qui s'inscrit dans le chantier législatif plus vaste de l'entrée de la France dans la société de l'information.

Assemblée nationale, 13 mars 2000, n° 11 (p. 1672)

21754 — 6 janvier 2000. — **M. Michel Moreigne** attire l'attention de **M^me^ le ministre de la Culture et de la Communication** sur la régulation du réseau Internet au plan national. L'instauration de cadres réglementaires et déontologiques n'entravant pas le développement du « Web » paraît nécessaire. Il lui demande donc si la création d'une nouvelle autorité administrative de régulation d'Internet et des réseaux numériques d'information est envisagée ou si les instances de régulation actuelle (Conseil supérieur de l'audiovisuel et Autorité de régulation des télécommu-

nications) se verront attribuer des compétences nouvelles élargissant au réseau précité le domaine d'intervention qui leur est propre. En outre, il lui demande si un projet de loi est en préparation sur ce point précis.

Réponse. — Le droit positif a vocation à s'appliquer sur l'Internet, notamment les règles relatives à la liberté des consommateurs ou de la vie privée. Toutefois, les spécificités du réseau, son caractère décentralisé et sa dimension planétaire peuvent rendre difficile l'application de ce droit. Le développement de l'autorégulation, permettant l'élaboration et le respect de règles déontologiques par les acteurs eux-mêmes ; paraît pouvoir contribuer ainsi à la prévention des comportements préjudiciables. ◦ la suite des normes de comportements dites « netiquette » fixées par les utilisateurs aux origines de l'Internet, divers acteurs ont été amenés à définir des pratiques et usages à l'instar de l'Association des fournisseurs d'accès (AFA). Diverses instances ont parallèlement tenu à préciser certaines normes ou à prononcer des avis couvrant des aspects particuliers de l'Internet relevant du champ de compétence de chacune de ces autorités. Ainsi en est-il notamment de l'Autorité de régulation des télécommunications (ART), de la Commission nationale de l'informatique et des libertés (CNIL), ou bien encore de la Commission des opérations de bourse (COB). Les règles définies par les acteurs complètent, sans s'y substituer, les dispositifs législatifs et réglementaires et l'intervention des pouvoirs publics. Sur cette base, il paraît souhaitable et possible de développer une « co-régulation », suscitant une coopération approfondie entre les pouvoirs publics, les usagers et les entreprises. Dans le cadre de la consultation relative au cadre juridique de la société de l'information, le gouvernement a souligné que la nature même de l'Internet ne conduisait pas à en confier la régulation à une autorité administrative indépendante spécifique. Il a en revanche indiqué qu'il envisageait la mise en place d'un organisme associant acteurs publics et privés dans un but de concertation et de déontologie. Le Premier ministre a, dans cet objectif, souhaité confier une mission de réflexion au député Christian Paul afin de tracer, en consultant l'ensemble des acteurs, les grandes lignes d'un éventuel organisme, les compétences susceptibles de lui être dévolues ainsi que les modalités de son fonctionnement.

Sénat, 9 mars 2000, n° 10 (p. 864)

Publicité et publipostage

20931 —2 décembre 1999. — Le chiffre d'affaires du marché publicitaire sur Internet est en constante augmentation - 284 % entre 1997 et 1998. Alors que certaines personnes regroupées en « communautés virtuelles » acceptent de fournir des renseignements personnels pour accéder à des services gratuits moyennant l'affichage de multiples publicités sur leurs écrans, d'autres internautes, sans avoir donné leur accord, font l'objet d'intrusions publicitaires de plus en plus fréquentes sans pouvoir s'y soustraire. Les particuliers sont en fait soumis à une surveillance, rapprochée de la part des publicitaires, qui observent le contenu de leurs messages électroniques, et le parcours qu'ils empruntent. Des « mouchards » permettent en effet d'identifier chaque ordinateur et de cibler ensuite les internautes en fonction de leurs pôles d'intérêt. Face à la multiplicité de ces pratiques publicitaires abusives, plusieurs États américains ont adopté des mesures interdisant aux annonceurs d'expédier des messages publicitaires, à moins que leurs destinataires n'aient préalablement accepté d'en recevoir. En Europe, la directive communautaire du 20 mai 1997, relative aux contrats à distance, prévoyait déjà une obligation d'identification de toute publicité de ce type. La Commission européenne, dans sa proposition de directive n° 98-586 sur le commerce électronique, impose aux États membres de prévoir, dans leur légis-

lation, que la communication commerciale par courrier électronique non sollicitée, soit identifiée comme telle, d'une manière claire et non équivoque, dès sa réception par le destinataire. Cependant, cette proposition, contrairement à la décision américaine, met à la charge de l'internaute le soin de s'opposer aux messages non sollicités. L'Autriche, l'Italie et la Belgique, profitant de la faculté pour les États membres de la Communauté européenne de prévoir une réglementation plus sévère, ont d'ores et déjà adopté des textes imposant que le consentement du destinataire de publicité par courrier électronique ait été préalablement recueilli. **M. José Balarello** demande à **M^me^ le ministre de la Culture et de la Communication** quelles mesures elle entend prendre afin de limiter le développement anarchique de ces pratiques qui portent atteinte à la vie privée de nos concitoyens. L'envoi en masse des publicitaires contribuant, par ailleurs, à augmenter le trafic sur Internet et donc à ralentir les transmissions.

Réponse. — Il est indéniable que certaines pratiques de prospection commerciale sur Internet sont susceptibles de porter atteinte à la vie privée des personnes et participent à l'encombrement du réseau. Conscient de cet état de fait et face au caractère incomplet de la réponse apportée par le droit positif, le gouvernement a soumis à consultation dans le document d'orientation relatif au futur projet de loi « Société de l'information » les grandes lignes d'adaptation du cadre législatif et réglementaire français dont un volet appréhende la question de la généralisation du traitement des données dans l'environnement des services en ligne. Conformément aux principes posés par la directive du 24 octobre 1995, il importe de maintenir et de renforcer les principes fondamentaux de la loi du 6 janvier 1978 dite « Informatique et libertés ». Le projet renforce, en lui conférant un caractère discrétionnaire, le droit d'opposition des personnes lorsque le traitement de leurs données personnelles est effectué à des fins de prospection ou d'information publicitaire. Ce texte devrait conforter les garanties actuellement reconnues aux abonnés et utilisateurs des réseaux ou services de télécommunications leur permettant d'interdire que des informations nominatives les concernant soient utilisées dans des opérations commerciales (listes orange et safran). En outre, il peut être souligné que la Commission nationale de l'informatique et des libertés, dans un rapport d'octobre 1999 sur « La prospection non sollicitée sur l'Internet et le spamming », a rappelé les règles fondamentales à respecter. La CNIL réaffirme notamment que les messages électroniques figurant dans les espaces publics de l'Internet ne peuvent être collectés à des fins de prospection à l'insu des internautes et souhaite à cet effet encourager les chartes et codes de bonne conduite des organismes professionnels.

Sénat, 25 mai 2000, n° 21 (p. 1852)

Accès à la jurisprudence

48280 — 3 juillet 2000. — **M. Yves Coussain** attire l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur les difficultés rencontrées par les justiciables pour avoir accès à la jurisprudence en vigueur. En effet, la jurisprudence représente à l'heure actuelle une part fondamentale du droit positif. Or, contrairement aux textes de loi ou réglementaires publiés au *Journal officiel* et diffusés très largement sur les sites Internet et officiels des pouvoirs publics, la jurisprudence ne fait l'objet d'aucune publication officielle, rapide et systématique. Certaines décisions de jurisprudence ne sont même jamais publiées. ◦ l'heure actuelle, les seules sources d'informations automatisées permettant des recherches thématiques fiables et rapides dont disposent les justiciables sont des bases de données privées, très onéreuses et pas toujours exhaustives ; les jugements de première instance y figurent no-

tamment rarement. La connaissance de la jurisprudence étant déterminante dans l'issue de beaucoup de procès, il semble anormal qu'aucun accès n'y soit organisé par les pouvoirs publics au bénéfice des justiciables. Il lui rappelle que parallèlement, la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations prévoit, comme principe général, que les autorités administratives sont tenues d'organiser un accès simple aux règles qu'elles édictent, et que la mise à disposition et la diffusion des textes juridiques constituent une mission de service public. Il serait bon que ce principe puisse être étendu à la jurisprudence, et ce d'autant qu'à l'heure de la société de l'information, le gouvernement a manifesté la volonté de promouvoir par Internet une information simple et élargie du public. A cet égard, il semblerait notamment que des Intranet existent entre les juridictions, tant privées que publiques, sur lesquelles la plus grande partie de la jurisprudence serait disponible, mais laissée à l'utilisation exclusive des magistrats. En conséquence, il lui demande quelles mesures elle entend prendre afin d'organiser un égal accès à la jurisprudence des justiciables.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'elle attache le plus grand intérêt à la diffusion sur Internet des données publiques concernant la jurisprudence, tant des juridictions nationales qu'européennes, qui constitue un outil complémentaire de connaissance et d'interprétation des textes juridiques. Il s'agit là d'une mission de service public de nature à donner pleine effectivité aux droits des citoyens, notamment dans leurs relations avec les administrations, tels que posés par la loi n° 2000-321 du 12 avril 2000, et à favoriser l'égal accès de tous les justiciables à la justice. Le gouvernement a créé, par le décret n° 84-940 du 24 octobre 1984, le service public des bases et banques de données juridiques et placé auprès du Premier ministre le Centre national d'informatique juridique dont les activités ont ensuite été reprises par la direction des *Journaux officiels.* Ce service public a été réorganisé par le décret n° 96-481 du 31 mai 1996 et la base de données élargie à la jurisprudence du Conseil constitutionnel, du tribunal des conflits, de l'ensemble des juridictions administratives, judiciaires et financières ainsi qu'à celles des juridictions européennes ; la diffusion assurée, depuis le 1er janvier 1992, par la société ORT, titulaire de la concession du service public des bases de données juridiques, permet aujourd'hui d'accéder dans le cadre de deux services distincts, d'une part, gratuitement, sous la marque Legifrance à « l'essentiel du droit français » et, notamment, à une sélection de la jurisprudence des juridictions suprêmes, et, d'autre part, sur le site payant Jurifrance, à un service documentaire et professionnel exhaustif, en particulier pour la jurisprudence. La diffusion gratuite sur l'Internet des données publiques les plus utiles aux citoyens et aux entreprises, qui apparaît une exigence démocratique, constitue une des priorités fixées par le Premier ministre à l'action gouvernementale à l'occasion de son discours prononcé à Hourtin en août 1997. Cet objectif, inscrit dans la démarche globale du programme d'action gouvernemental pour la société de l'information (PAGSI), s'est enrichi des conclusions du rapport remis en novembre 1999 par M. Dieudonné Mandelkern, *Diffusion des données publiques et révolution numérique,* qui recommande une diffusion gratuite et exhaustive des données juridiques. Le gouvernement entend donner suite à cette recommandation en offrant, à terme, un service en ligne de données juridiques exhaustif et gratuit. Ce site, qui permettra à tout citoyen d'accéder à l'ensemble de la jurisprudence, conformément à la décision prise lors du comité interministériel pour la réforme de l'État du 12 octobre 2000, sera mis en place dès qu'auront été réglés les aspects techniques, organisationnels, documentaires ou tenant, par exemple, à l'anonymisation des données.

Assemblée nationale, 20 novembre 2000, n° 47 (p. 6634)

JUSTICE

Fichier génétique

35633 — 11 octobre 1999. — **M. Gérard Voisin** appelle l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur la mise en place du fichier génétique national. Il relève que, malgré les assurances formulées en novembre 1998 par le gouvernement sur cette question, le fichier génétique national n'est toujours pas en service. Il note, en effet, que la Commission nationale de l'informatique et des libertés n'a été saisie de ce dossier que dans le courant de l'été 1999. Il demande donc au gouvernement de lui préciser les délais prévisibles pour la mise en place effective de cet outil efficace et attendu.

Réponse. Le Garde des Sceaux, ministre de la Justice, a l'honneur d'indiquer à l'honorable parlementaire que depuis le vote de la loi du 17 juin 1998 la création du fichier national automatisé des empreintes génétiques a constitué une priorité de son action. Cependant, la création de ce fichier représente une nouveauté technique considérable qui a nécessité de procéder à une concertation approfondie entre les différents ministères concernés. Ce travail préparatoire, qui explique les délais d'élaboration du décret, a permis de fixer les modalités de fonctionnement concrètes du fichier ainsi que les garanties qui doivent l'entourer pour respecter la loi. Les segments d'ADN sur lesquels porteront les analyses, qui feront l'objet d'un arrêté interministériel, ont ainsi été choisis de telle sorte qu'ils soient en conformité avec les recommandations internationales de manière à assurer une compatibilité des différents fichiers nationaux, et qu'ils soient non codants, c'est-à-dire qu'ils ne révèlent pas d'informations discriminantes sur des anomalies génétiques de la personne. Par ailleurs, il a été décidé, pour des raisons à fa fois d'efficacité et de sécurité, de centraliser le stockage des prélèvements qui font l'objet d'analyse d'empreinte génétique au sein d'un service central de préservation des prélèvements biologiques créé par le décret à cet effet. Enfin, les méthodes d'enregistrement et de traitement des informations ont été élaborées pour présenter les garanties de viabilité et de sécurité indispensables. Ce travail sur les garanties que devait offrir le projet de décret portant création du fichier national automatisé des empreintes génétiques s'est avéré décisif pour obtenir l'avis le 2 novembre 1999 par la CEIL. Après les dernières concertations interministérielles nécessaires, le projet a été transmis au Conseil d'État le 31 janvier 2000. Le décret devrait ainsi pouvoir être publié dans les prochaines semaines et le fichier entrera en fonctionnement dans le premier semestre de l'année 2000 compte tenu des dernières mises au point techniques qui restent à effectuer. Enfin, il convient de rappeler que, afin de pouvoir alimenter le fichier dès son entrée en fonction et de commencer immédiatement à opérer des rapprochements, une circulaire diffusée le 14 décembre 1998 aux procureurs généraux donnait pour instruction de faire pratiquer des expertises aux fins de recueillir les empreintes génétiques des personnes mises en cause dans toutes les procédures concernant des infractions sexuelles.

Assemblée nationale, 17 avril 2000, n° 16 (p. 2487)

41**754** — 14 février 2000. — **M. Jean-Luc Warsmann** attire l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur le décret d'application relatif à la loi sur la délinquance sexuelle. Deux mesures importantes de la loi sur la délinquance sexuelle de juin 1998 ne peuvent être mises en place. En effet, juges, policiers et gendarmes attendent toujours l'installation du fichier national d'empreintes génétiques qui leur permettrait d'identifier rapidement les auteurs de viols ou d'agressions sexuelles. De même, depuis 1998, les tribunaux peuvent condamner un délinquant sexuel à se soigner pendant une période de cinq à dix ans après sa sortie de prison. Toutefois, les décrets d'application n'ont toujours pas été pris. Il souhaite-

rait donc savoir quand le gouvernement entend prendre les décrets d'application afin de permettre une application effective des dispositions de la loi sur la délinquance sexuelle.

Réponse. — Le Garde des Sceaux, ministre de la Justice, a l'honneur d'indiquer à l'honorable parlementaire que les décrets d'application de la loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, ont tous été publiés. En particulier, le décret n° 2000-413 du 18 mai 2000 relatif au fichier national des empreintes génétiques et au service central de préservation des prélèvements biologiques, fixe les modalités concrètes de fonctionnement du fichier ainsi que les garanties qui l'entourent. Par circulaire du 10 octobre 2000, instruction a été donnée aux procureurs de la République de commencer à alimenter le fichier en adressant les empreintes génétiques des personnes condamnées pour infractions sexuelles ainsi que les analyses génétiques des traces relevées au cours des enquêtes, au service de la direction de la police judiciaire qui a en charge le fonctionnement du fichier. Cette base de donnée de comparaison sera intégrée immédiatement au fichier lorsque, dans quelques mois, celui-ci sera opérationnel et permettra ainsi d'effectuer des rapprochements utiles. En ce qui concerne les dispositions relatives au suivi socio-judiciaire, le décret n° 99-571 du 7 juillet 1999 a introduit, dans le livre V du code de procédure pénale, un titre V qui précise la procédure applicable en la matière. Par ailleurs, le décret n° *2000-4*12 du 18 mai 2000 a inséré dans le livre III du code de la santé publique un titre IX relatif à l'injonction de soins concernant les auteurs d'infractions sexuelles, qui prévoit les modalités de constitution des listes de médecins coordonnateurs, ainsi que la procédure de leur désignation. Les modalités de choix du médecin traitant et du déroulement de l'injonction de soin y sont également précisées. Deux arrêtés fixant la rémunération des médecins coordonnateurs et le nombre de condamnés qu'ils peuvent suivre chaque année seront publiés dans les semaines à venir. Par conséquent, le cadre juridique résultant des décrets nécessaires au fonctionnement de ces deux nouveaux moyens de lutter contre les infractions sexuelles que constituent le fichier des empreintes génétiques d'une part, et le suivi socio-judiciaire d'autre part, est aujourd'hui pratiquement achevé.

Assemblée nationale, 27 novembre 2000, n° 48 (p. 6754)

Données conservées par les juridictions

23193 — 2 mars 2000, — **M. Michel Dreyfus-Schmidt** attire l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur les potentialités discriminatoires issues de la rédaction du décret 90-115 du 2 février 1990 portant application aux juridictions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'article 31 de la loi susmentionnée, ainsi modifiée, autorise, pour l'exercice de leur mission, les juridictions de l'ordre judiciaire et de l'ordre administratif, à mettre ou conserver en mémoire informatisée les données nominatives qui font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales. Le caractère extrêmement sensible des données enregistrées sur un support informatique — dont la finalité peut toujours être détournée —, présente un risque évident pour la vie privée des personnes. C'est pourquoi assurément, dans des décrets récents, notamment le décret n° 99-1091 du 21 décembre 1999 relatif au pacte civil de solidarité, le gouvernement a pris la précaution d'insérer un article interdisant expressément de sélectionner une catégorie de personne à partir des données récoltées, garantissant par là même le caractère privé de la sexualité des

partenaires concernés. Précaution absente du décret 90-115, du 2 février 1990. Il lui demande donc si la sécurisation juridique du décret passant par l'interdiction expresse de l'utilisation de la base de donnée en vue de la sélection d'une catégorie de personne, ne pourrait venir utilement compléter le dispositif actuel de l'article 31 de la loi susvisée.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que les risques présentés par une catégorie de traitements de données nominatives au regard des droits et libertés des personnes doivent être appréciés *in concreto,* compte tenu de la finalité de ces traitements ainsi que de la nature et de l'étendue des données traitées. Outre le fait que la procédure dans le cadre de laquelle ce texte a été pris offre de nombreuses garanties, puisqu'elle suppose notamment un avis conforme de la Commission nationale de l'informatique et des libertés, il importe d'observer que le décret n° 90-115 du 2 février 1990 portant application aux juridictions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne confère aux juridictions aucune habilitation générale à mettre ou conserver en mémoire informatisée des données de la nature de celles visées par cette disposition. En effet, ce décret, d'une part, ne concerne que les « données nominatives nécessaires à l'instruction et au jugement des litiges (...) et à l'exécution des décisions de justice » et, d'autre part, n'est susceptible de trouver application qu'à des traitements mis en œuvre « pour l'exercice des missions des juridictions ». Il est de surcroît nécessaire que ceux-ci aient satisfait aux formalités de l'article 15 de la loi susvisée du 6 janvier 1978, lesquelles supposent un examen préalable par la CNIL et un acte réglementaire du gouvernement. En pratique, le décret du 2 février 1990 permet essentiellement aux juridictions judiciaires et administratives d'induire dans des traitements de gestion interne de leurs dossiers des données d'une nature sensible que les parties sont appelées à communiquer pour définir leur qualité, déterminer l'objet du litige ou aider à sa résolution. En tout état de cause, les risques de sélection à des fins de discrimination qui s'attachent à ces traitements ne peuvent être considérés comme du même ordre que ceux qui découlent, s'agissant de fichiers non placés directement sous la responsabilité de l'autorité judiciaire et susceptibles de révéler indirectement les orientations sexuelles des personnes qu'ils concernent, de la conservation des données relatives au pacte civil de solidarité et qui expliquent l'introduction dans le décret n° 99-1091 du 21 décembre 1999 d'une disposition spécifique prohibant expressément toute sélection d'une catégorie particulière de personnes. Compte tenu de ces éléments, il n'est pas envisagé de modifier le décret du 2 février 1990, les garanties offertes par celui-ci apparaissant conformes à la loi et à nos obligations internationales.

Sénat, 7 septembre 2000, n° 35 (p. 3098)

Bracelet électronique

21355 — 16 décembre 1999.**—M. Emmanuel Hamel** attire l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur un des documents de travail du Sénat — série Législation comparée — intitulé « La lutte contre la délinquance juvénile », paru le 24 mars 1999 et dans lequel il est indiqué, à la page 13, qu'en Angleterre les jeunes de plus de dix-huit ans condamnés à une courte peine de prison peuvent bénéficier d'une libération conditionnelle assortie du port obligatoire d'un bracelet électronique. Il la remercie de bien vouloir lui indiquer son avis sur l'application d'une telle disposition en France. Le gouvernement français entend-t-il suivre un tel exemple ?

Réponse. — La Garde des Sceaux, ministre de la Justice a l'honneur de faire connaître à l'honorable parlementaire que la loi n° 97-1159 du 19 décembre 1997 a créé la possibilité de faire exécuter les courtes peines d'emprisonnement sous le régime du placement sous surveillance électronique. L'article 723-7 du code de procédure pénale dispose que le juge de l'application des peines peut ordonner d'office ou sur demande du procureur de la République le placement d'un condamné, après que son consentement a été recueilli en présence de son avocat, sous surveillance électronique, pour l'exécution d'une peine d'emprisonnement ou d'un reliquat de peine d'emprisonnement n'excédant pas un an. Cette décision peut être également prise à titre probatoire de la libération conditionnelle pour une durée n'excédant pas un an. L'article 20-8 de l'ordonnance du 2 février 1945 prévoit que la mesure est également applicable aux mineurs. La loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes a du reste précisé que, pour ces derniers, le juge devait obtenir l'accord des titulaires de l'autorité parentale. Contrairement à l'exemple britannique cité par l'honorable parlementaire, le placement sous surveillance électronique ne constitue pas une mesure de surveillance d'un condamné bénéficiant d'une libération conditionnelle. Il peut simplement être employé comme un essai préalable avant l'octroi d'une telle mesure quel que soit le reliquat de la peine restant à subir. Il convient de rappeler que dans l'intention du législateur, comme cela a été unanimement exposé dans les débats parlementaires, la mesure de placement sous surveillance électronique doit notamment permettre à davantage de condamnés d'exécuter les peines d'emprisonnement de courtes durées en dehors des établissements pénitentiaires. Dans cette finalité, elle ne doit pas être utilisée pour des condamnés qui auraient, quoi qu'il en soit, bénéficié d'une libération conditionnelle, mais, au contraire, elle devrait être appliquée à une partie de la population pénale à laquelle la libération conditionnelle n'est pas octroyée. Par ailleurs, lorsqu'elle précède à titre probatoire une mesure de libération conditionnelle, elle peut favoriser l'accès à celle-ci à des condamnés pour lesquels cette solution n'aurait pas été envisagée. Ainsi appliqué, le placement sous surveillance électronique est susceptible de représenter une modalité d'exécution de la peine très utile pour des jeunes majeurs ou des mineurs contre qui il a été nécessaire de prononcer une peine d'emprisonnement ferme mais pour lesquels il est ainsi possible d'éviter les effets néfastes de l'emprisonnement qui sont particulièrement marqués pour ces détenus. Une expérimentation portant sur le placement sous surveillance électronique a débuté dans quatre sites, à Aix-en-Provence, Agen, Grenoble et Lille, avant de procéder à la généralisation du dispositif. Par conséquent, l'effet de cette mesure et sa place dans le traitement de la délinquance juvénile ne pourront être appréciés immédiatement et devront faire l'objet d'une analyse après plusieurs mois d'application de cette disposition sur l'ensemble du territoire.

Sénat, 28 décembre 2000, n° 51 (p. 4490)

LIBERTÉS PUBLIQUES

Transposition de la directive 95/46/CE

31112—7 juin 1999. — **M. Bernard Accoyer** attire l'attention de **M. le ministre délégué chargé des Affaires européennes** sur la non-transposition en droit français de la directive n° 95-46 relative au traitement des données et à leur libre circulation et qui aurait dû être effectuée avant le mois d'octobre 1998. Alors que le gouvernement disposait d'un rapport sur les modalités de cette transposition rédigé par M. Guy Braibant, aucune disposition législative n'a été à ce jour déposée à cette fin au Parlement, si ce n'est un article spécifique relatif au programme de mé-

dicalisation du système d'information (PMSI) dans le projet de loi portant création de la couverture maladie universelle. Une phase pré-contentieuse vient d'être ouverte à l'encontre de la France pour non transposition de cette directive. C'est la raison pour laquelle il lui demande de bien vouloir lui indiquer la conduite que le gouvernement français envisage de tenir en ce domaine. ***Question transmise à M^me^ le Garde des Sceaux, ministre de la Justice.***

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que 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 devait être transposé en droit national dans un délai de trois ans après son adoption. Le retard pris dans cette transposition s'explique, outre par le changement de gouvernement intervenu au printemps 1997, par la nécessité d'adapter le régime actuel aux bouleversements considérables qui ont affecté depuis 1978 la place tenue par l'informatique dans la société contemporaine, en tenant compte de la circulation accrue que connaissent aujourd'hui les données à caractère personnel et de l'exigence de préserver un niveau élevé de protection des droits fondamentaux des personnes. Ces exigences ont rendu indispensables une réflexion et des travaux préparatoires de grande ampleur. S'il convient de souligner à cet égard le rôle déterminant du rapport intitulé *Données personnelles et société de l'information,* remis au Premier ministre en mars 1998, des études complémentaires sur des problèmes que la mission Braibant n'avait pas pour mission de traiter ont dû être menées par ailleurs courant 1997 et 1998. Il en va ainsi notamment de l'étude du Conseil d'Etat sur Internet et les réseaux numériques, rendue publique à l'automne 1998. C'est en s'appuyant sur ces différents travaux que la chancellerie a élaboré un avant-projet de loi de transposition, dont l'examen interministériel est aujourd'hui achevé mais qui doit encore être soumis, pour avis, conformément aux dispositions en vigueur pour des projets qui touchent à la protection des libertés individuelles, à la Commission nationale informatique et libertés (CNIL) et à la Commission nationale consultative des droits de l'homme (CNCDH). Le projet de loi, éventuellement complété afin de tenir compte des avis de ces deux instances consultatives, sera alors soumis au Conseil d'État, puis examiné en Conseil des ministres. Ainsi, le Parlement pourra-t-il être saisi à bref délai de ce texte auquel le gouvernement attache une très grande importance et qui s'inscrit dans le chantier législatif plus vaste de l'entrée de la France dans la société de l'information.

Assemblée nationale, 28 février 2000, n° 9 (p. 1340)

Ficher Europol

37555 — 22 novembre 1999. — **M. Patrick Bloche** attire l'attention de **M. le ministre de l'Intérieur** sur l'utilisation des données contenues dans le fichier d'Europol. L'internationalisation des réseaux criminels nécessite la mise en place de moyens adaptés et performants au service des polices européennes. ◦ titre d'exemple, la France met à la disposition d'Europol, depuis peu, un fichier comportant une liste des personnes mises en examen ou simples témoins dans des affaires judiciaires. Chaque pays élabore son fichier selon ses pratiques et ses propres législations. Or certains pays de l'Union européenne ont constitué des fichiers comportant des informations strictement personnelles, comme les pratiques religieuses ou sexuelles. Même si la France ne transmet pas ce type d'informations, elle y a, de fait, accès. En conséquence, il souhaiterait savoir quelles assurances nous pouvons avoir qu'aucune de ces données ne sera susceptible d'être utilisée en France, et dans quelle mesure la France ne sera pas amenée à uniformiser ses fichiers en ce sens.

Réponse. — Europol est un office européen de police. La convention qui l'a instituée, signée le 26 juillet 1995 et entrée en vigueur le 1er juillet 1999, lui donne pour mission la lutte contre le terrorisme, le trafic illicite de stupéfiants et toutes les formes de criminalité internationale : trafic de matières nucléaires et radioactives, trafic de véhicules volés, lutte conte le faux-monnayage et la falsification des moyens de paiement, filières d'immigration clandestine, traite des êtres humains. Europol ayant pour principale fonction de faciliter les échanges d'informations entre les États membres de l'Union européenne, de collecter, rassembler et analyser des informations et des renseignements, de mettre à jour les liens constatés entre des faits délictueux et différents pays, de faciliter les enquêtes des États membres en leur fournissant les informations qui les concernent, il gère à cet effet un système informatisé d'informations, comprenant, d'une part, un système d'informations et, d'autre part, des fichiers de travail à des fins d'analyse, qui est alimenté directement par les États membres, représentés par leurs Unités nationales Europol et les officiers de liaison, dans la stricte observation de leurs procédures nationales (art. 7-1. de la convention). Au sein de chaque État membre, c'est l'Unité nationale qui est responsable de la communication avec le système d'informations (sécurité, délais de conservation des données). Au sein d'Europol, le droit d'accès au système d'informations Europol, pour introduire des données ou en rechercher, est réservé aux officiers de liaison de chaque État membre, aux directeurs et directeurs-adjoints d'Europol ainsi qu'aux agents de l'office dûment habilités. En particulier, la transmission de données par les Unités nationales ou les officiers de liaison vers le système Europol n'est possible que si le droit national de l'État membre autorise leur traitement aux fins de la prévention, de l'analyse ou de la lutte contre les infractions (art. 10-3 de la convention). La collecte éventuelle et le stockage de données relatives aux pratiques religieuses ou sexuelles ne peuvent donc être réalisés que pour l'accomplissement de l'une des finalités confiées à Europol et ces données doivent être en rapport avec la criminalité recherchée. Par ailleurs, l'utilisation des données à caractère personnel qui peuvent être extraites du système d'informations ou des fichiers d'analyse ne peut se faire que dans le respect du droit de l'État membre dont relèvent les services utilisateurs (art. 17-1, paragraphe 2, de la convention) et sous le contrôle des autorités nationales de contrôle. Pour ce oui concerne la France, notre pays n'alimente à ce jour que les fichiers d'analyse d'Europol. Mais en aucun cas les données communiquées ne proviennent d'une alimentation directe des fichiers nationaux, ces données n'étant envoyées à Europol qu'au coup par coup. ◦ l'inverse, la France peut avoir accès à des données dites sensibles, mais cet accès n'est possible que par le filtre des officiers de liaison français à Europol et par celui de l'Unité nationale, qui sont chargés de veiller au respect des prescriptions nationales, et ces données ne peuvent être utilisées que pour autant que notre législation le permet.

Assemblée nationale, 14 février 2000, n° 7 (p. 1044)

Réseau Échelon

42879 — 6 mars 2000. — **M. Jean-Luc Warsmann** attire l'attention de **M. le Premier ministre** au sujet du réseau anglo-saxon Échelon d'espionnage des télécommunications au niveau mondial. Le débat au Parlement européen sur le réseau Échelon a suscité de nombreux échos en Europe et en France. De nouvelles preuves seraient apparues selon lesquelles une partie de la vocation de ces installations est commerciale alors que le gouvernement américain fait traditionnellement valoir des impératifs de défense. Selon cette étude, le réseau Échelon permettrait d'intercepter dans le monde entier les communications transmises par voie satellitaire, qu'il s'agisse de messages téléphoniques, de fax ou de courrier électronique via Internet. Aussi, il souhaiterait connaître la position du gouvernement sur cette étude et les

moyens qu'entend mettre en œuvre le gouvernement pour assurer la sécurité des communications. — ***Question transmise à M. le ministre de la Défense.***

Réponse. — Le « réseau Échelon de surveillance et d'interception des télécommunications à l'échelle mondiale » a été mis en place, à l'origine, pour des raisons de sécurité militaire. Selon deux rapports remis au Parlement européen, il aurait été utilisé à des fins d'espionnage économique. Face à ce possible détournement d'objectif, le Parlement européen, dans une résolution de septembre 1998, a appelé à la mise en place de systèmes de contrôle public et à l'adoption de mesures de cryptage et de protection des informations économiques. Le recueil d'informations dans un objectif de sécurité nationale a toujours été nécessaire. Cependant, l'accroissement des échanges de données et des réseaux d'informations multiplie les risques d'interception, de piratage de données sensibles ou d'atteintes à la vie privée. De plus, l'interconnexion de ces réseaux ouverts avec les réseaux internes des entreprises renforce les possibilités d'accès parasites à des informations sensibles. Pour se prémunir de tels risques, chaque pays s'est doté d'une législation visant à protéger les atteintes à la vie privée. En ce qui concerne la France, l'article 226-1 du code pénal punit « d'un an d'emprisonnement et de 300 000 francs d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui, en captant, enregistrant ou transmettant sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ». Par ailleurs, la loi — du 10 juillet 1991 relative au secret des correspondances émises par les télécommunications garantit, en son article I^{er}, les particuliers contre les interceptions opérées hors du cadre de cette loi. Elle institue notamment une Commission nationale de contrôle des interceptions de sécurité, qui peut être saisie par toute personne y ayant un intérêt direct et personnel. Au-delà de ces barrières juridiques, il est indispensable que les administrations et les entreprises développent une culture de protection de l'information sensible, en particulier dans le cas d'un transfert par satellite de rediffusion. Dans ce cadre, le ministre de la Défense a nommé un directeur de la sécurité des systèmes d'information qui assure la coordination des politiques de sécurité de tous les états-majors, services et directions de son ministère. D'autres initiatives concernant le secteur civil ont été prises par le gouvernement. Ainsi, lors du comité interministériel du 19 janvier 1999, le Premier ministre a annoncé une modification du cadre législatif français en matière de cryptologie visant à offrir une liberté complète dans l'utilisation des moyens de chiffrement utilisant des clés allant jusqu'à 128 bits, ce qui constitue un niveau qui permet d'assurer durablement une grande sécurité. De plus, le gouvernement a décidé, au début de cette année, de mettre en place un centre de veille, de prévention et de secours chargé de coordonner les efforts des administrations pour faire face aux attaques informatiques. C'est dans cette optique qu'une direction de la sécurité des systèmes d'information auprès du Premier ministre a été créée. Par ailleurs, des mesures complémentaires de protection des informations industrielles sont également à l'étude et seront soumises d'ici à quelques mois au Parlement.

Assemblée nationale, 15 mai 2000, n° 20 (p. 2991)

POLICE *STIC*

31369 — 14 juin 1999. — **M. Jean Rouger** souhaite attirer l'attention de **M. le ministre de l'Inférieur** sur le système de traitement des infractions constatées (STIC). Il convient de souligner, en effet, que la constitution de ce fichier a suscité de vives interrogations au sein de la CNIL jusqu'à son adoption en 1998. Même s'il

n'est plus question désormais d'y adjoindre les victimes ou les témoins des délits et des crimes, même si son accès s'est vu réservé aux officiers de police judiciaire et aux personnes habilitées par la direction générale de la police nationale, il n'en demeure pas moins que le STIC semble véhiculer les germes d'une suspicion généralisée contre la présomption d'innocence. C'est la raison pour laquelle il lui demande de bien vouloir préciser les garanties qui peuvent être apportées dans la mise en place de ce système.

Réponse. L'instruction de l'avis sur la mise en œuvre du système de traitement des infractions constatées (STIC) est en cours devant la Commission nationale de l'informatique et des libertés, et le ministère de l'Intérieur poursuit des discussions avec cette autorité administrative indépendante pour que, dans le respect des libertés et des besoins de l'ordre public, les garanties maximales soient offertes par cette application en ce qui concerne les préoccupations évoquées par l'honorable parlementaire.

Assemblée nationale, 28 août 2000, n° 35 (p. 5078)

Identification des voitures volées

26537 — 6 juillet 2000. — **M^me^ Marie-Claude Beaudeau** attire l'attention de **M. le ministre de l'Intérieur** sur la nécessité d'une identification sélective des véhicules volés fonctionnant au GPL. Elle lui souligne les risques d'explosion imprévisibles de ces véhicules auxquels sont exposés notamment les sapeurs pompiers lorsqu'ils interviennent lors de feux de voitures. L'explosion d'un véhicule GPL peut se traduire en effet par la projection par effet « missile » de parties du véhicule à plusieurs dizaines de mètres. Elle lui rappelle que les sapeurs-pompiers interviennent chaque jour sur de nombreux véhicules incendies légers et qu'un grand nombre de véhicules incendiés sont des véhicules volés. Plusieurs explosions dramatiques de véhicules GPL ont déjà eu lieu ou ont été évitées de justesse dans ces circonstances. Elle lui demande quelles dispositions prendre pour que les vols de véhicules GPL soient spécialement enregistrés par les services de police ou de gendarmerie et que les pompiers soient, le plus rapidement possible, informés de l'identité de ces véhicules. ◦ cette occasion, elle lui demande également où en sont les évolutions de réglementation envisagées sur l'accès des véhicules GPL aux parkings en sous-sol et aux tunnels et sur des modifications techniques de leurs réservoirs en vue d'en accroître la sécurité.

Réponse. — Le fichier des véhicules volés FVV est alimenté à partir des déclarations de vol de véhicules par les services de la police et de la gendarmerie nationales. Il ne dispose d'aucun renseignement relatif à l'énergie utilisée par les véhicules. L'enrichissement de la base de données avec cet élément d'information complémentaire est techniquement réalisable. Il nécessiterait soit l'ajout dans la grille « avis de vol » d'une rubrique concernant l'énergie utilisée, soit la création d'une nouvelle passerelle entre le FVV et le fichier national des immatriculations FNI afin d'extraire, à partir du numéro minéralogique des véhicules volés, le contenu de la rubrique « énergie » figurant dans ce fichier. Au plan juridique, la rédaction actuelle de l'arrêté du 15 mai 1996 relatif au FVV ne permet pas l'accès des sapeurs-pompiers aux informations contenues dans ce fichier. La modification de ce texte réglementaire autorisant cette consultation nécessiterait le recueil préalable de l'avis conforme de la Commission nationale de l'informatique et des libertés. Outre cette contrainte juridique, le caractère non exhaustif des réponses qui pourraient être apportées, le cas échéant, par le FVV aux sapeurs-pompiers lors de leurs interventions sur des véhicules incendiés, constitue un obstacle majeur à la mise en œuvre d'une telle procédure. En effet, tous les véhicules incendiés ne sont pas forcément volés ou n'ont pas fait

l'objet d'une déclaration préalable à l'intervention urgente des services de secours. L'identification d'un véhicule volé ou non suppose de plus l'existence et la visibilité de sa plaque d'immatriculation au moment de l'intervention, cette dernière étant susceptible d'avoir été arrachée par les auteurs du vol ou simplement détruite par le feu. Enfin, la fiabilité de l'information communiquée aux sapeurs-pompiers demeure relative en présence d'un véhicule faussement immatriculé (utilisation d'une doublette) ou d'un véhicule dont les transformations du type d'énergie utilisée n'auraient pas été signalées aux autorités. La communication d'informations erronées aux services de secours aurait ainsi des conséquences contraires aux buts recherchés en termes de sécurité pour les personnels intervenants. Le FNI présente l'avantage de fournir d'ores et déjà tous les éléments distinctifs d'un véhicule dont le type d'énergie utilisée et, grâce à un échange informatisé avec FVV, il fournit également des informations en cas de véhicule signalé volé. L'élaboration d'un fichier spécifique ou l'alimentation d'une rubrique supplémentaire ne semblent ainsi pas opportuns, le FNI s'avérant une source de renseignements plus exhaustive pouvant, en partie et dans la mesure où les modalités d'accès à cette application auront été déterminées, répondre aux préoccupations légitimes des services de secours.

Sénat, 12 octobre 2000, n° 40 (p. 3490)

SANTÉ

Secret et informatisation

28149 — 12 avril 1999. **M. Jean-Paul Bref** appelle l'attention de **M. le secrétaire d'État à la Santé et à l'Action sociale** sur les conséquences de l'informatisation progressive des services des centres médico-psychologiques. La mise en réseau des structures de soin de la psychiatrie publique se traduit par des procédures de plus en plus préoccupantes en termes d'éthique, de déontologie et de libertés individuelles. En effet, les professionnels de la santé, conformément à la loi, remplissent des fiches nominatives sur chaque patient qui comportent, outre l'état civil, des données concernant la vie privée, le diagnostic et un recueil d'activités soignantes. Ces renseignements sont ensuite transmis par réseau au médecin responsable du département d'information médicale. Cette pratique, qui se traduit dans les faits par une délégation systématique du secret professionnel, tend à s'amplifier. Ce qui se fait à l'échelle d'un établissement se généralise et les transferts d'information ont lieu aujourd'hui entre les hôpitaux. Bientôt, les mises en réseau de la médecine de ville, de la sécurité sociale et des mutuelles accentueront plus encore le danger de fuites de données confidentielles. De nombreux professionnels sont inquiets et demandent une anonymisation à la source des données sensibles sur les patients. Il lui demande de bien vouloir lui donner son avis sur cette proposition.

Réponse. — L'honorable parlementaire souligne la nécessité de protéger les données sensibles à caractère médical dans un contexte de développement de l'informatisation de la santé. S'agissant des informations utilisées par les professionnels de santé dans le cadre direct de la prise en charge des patients et de l'administration de soins, il convient de rappeler que la sécurisation des systèmes d'information en réseau est une des priorités poursuivies par les pouvoirs publics ; le déploiement d'outils d'authentification des professionnels de santé et de chiffrement des messages est ainsi au cœur des projets relatifs au réseau santé social, à la carte Sesam-Vitale et à la carte de professionnel de santé. S'agissant de l'utilisation de données de santé à caractère personnel à des fins d'étude ou d'analyse, l'article 41 de la loi n° 99-641 du 27 juillet 1999, portant création d'une couverture maladie universelle, met en place une procédure d'autorisation sous le contrôle de la Commission nationale de

l'informatique et des libertés. Les informations communiquées selon cette procédure ne seront jamais directement nominatives puisque n'y figureront ni le nom ni le prénom ni le numéro d'inscription au répertoire national des personnes physiques. Le Conseil constitutionnel a validé ces dispositions protectrices de la vie privée des personnes.

Assemblée nationale, 7 février 2000, n° 6 (p. 916)

Secret et sida

18106 - 22 juillet 1999. — **M. Bertrand Delanoë** souhaite attirer l'attention de **M^me^ le ministre de l'Emploi et de la Solidarité** sur les risques de transgression du secret médical et de fichage de certaines données relatives à l'état de santé des malades du sida lors des procédures de mise en place de l'aide à domicile. Il semblerait ainsi que, dans plusieurs départements et notamment à Paris, des violations du secret médical aient été constatées et qu'un fichier comportant des données confidentielles sur l'état de santé des séropositifs du département ait été constitué. La DDASS (direction départementale des Affaires sanitaires et sociales) de Paris aurait même déposé une demande auprès de la CNIL (Commission nationale informatique et libertés) correspondant à la création d'un fichier relatif aux malades du sida bénéficiaires de l'aide à domicile. Il lui demande de faire toute la lumière sur ces possibles agissements. Il lui demande également de s'assurer que les nouvelles modalités mises en œuvre pour l'admission dans le dispositif de maintien à domicile et l'attribution des prestations d'aides à domicile sont bien conformes aux dispositions de la circulaire DGS/DS2 n° 96-10 du 8 janvier 1996 et ne sont pas susceptibles de provoquer des difficultés au regard du secret médical.

Réponse. — La circulaire du 8 janvier 1996 relative à l'aide à domicile aux patients atteints du VIH/Sida prévoit un dispositif départemental afin d'apporter aux personnes les prestations les plus adaptées possible à leur situation. Il appartient à un comité de pilotage, prévu dans chaque département, présidé par le préfet et composé notamment des associations intéressées et du ou des coordinateurs désignés, de faire des propositions sur l'organisation, la coordination et le financement départemental du dispositif. Quelques départements ont mis en place de leur propre initiative des commissions d'admission alimentées par l'évaluation des besoins des patients réalisée par les coordinateurs. Les directions départementales des Affaires sanitaires et sociales concernées, sollicitées à ce sujet, m'ont fait part des procédures mises en place pour ajuster les prestations aux besoins des patients. Aucun fichier nominatif n'a été mis en place. Lors des commissions d'admission, les dossiers sont traités de façon anonyme. En ce qui concerne Paris, les services de la DDASS ont réexaminé les modalités d'attribution des prestations à domicile des patients. Un certificat médical attestant que le malade peut bénéficier du dispositif de l'aide à domicile est établi par le médecin traitant à la demande du malade. Ce certificat lui est remis en main propre, à charge pour ce dernier de le transmettre à la coordination.

Sénat, 22 juin 2000, n° 25 (p. 2222)

38443 — 6 décembre 1999. — **M. François Asensi** attire l'attention de **M^me^ la ministre de l'Emploi et de la Solidarité** sur la remise en cause du principe d'anonymat dans le cadre de la surveillance épidémiologique du VIH-sida. Deux décrets parus au *Journal officiel,* du 16 mai 1999 instituent la possibilité d'une collecte d'informations nominatives sur les patients séropositifs. L'article R. 11-2 du décret n° 99-362 précise que « la notification des données individuelles est réalisée sous la forme d'une fiche qui comporte des éléments à caractère nominatif... ». De nombreuses associations de lutte contre le sida et de défense des droits de l'homme s'élèvent contre cette pratique instituant le fichage des personnes séropositives. Elle

brise le consensus oui s'était établi jusqu'à présent entre la communauté scientifique, les professionnels de la santé et les militants d'associations. Une surveillance épidémiologique rigoureuse et précise de l'épidémie de VIH et des autres maladies graves doit impérativement respecter le principe d'anonymat des personnes. Il souhaite recueillir son point de vue sur cette question. Il lui demande si elle envisage de mettre en place d'autres techniques de surveillance épidémiologique et de modifier ces décrets afin de garantir l'anonymat des données transmises à l'Institut de veille sanitaire.

Réponse. — La ministre de l'Emploi et de la Solidarité précise à l'honorable parlementaire que la loi du 1er juillet 1998 prévoit la déclaration obligatoire pour certaines maladies nécessitant des mesures de santé publique et de suivi épidémiologique. Deux décrets d'application ont été publiés le 6 mai 1999 : l'un définissant les règles de déclarations et la garantie de l'anonymat, l'autre fixant la liste des maladies qui font l'objet d'une déclaration obligatoire. Pour chacune de ces maladies, dont l'infection à VIH, les modalités de notification sont précisées par un arrêté spécifique. En juillet 1999, la mise en place de ce dispositif de déclaration a suscité des inquiétudes pour l'infection à VIH, de la part des associations. Compte tenu du très vif débat engagé autour du décret du 6 mai 1999 fixant les modalités de transmission de données individuelles à l'autorité sanitaire, plusieurs associations de défense des droits de l'homme et de lutte contre le sida estimant que l'anonymat des personnes n'était pas garanti, le gouvernement a chargé l'Institut de veille sanitaire, en novembre 1999, de constituer un comité de pilotage afin d'élaborer les modalités du système de surveillance de la séropositivité. En juin 2000, ce comité réunissant professionnels et associations a abouti à un dispositif consensuel. L'anonymat sera protégé par un hachage des données d'identification à la source. Un nouveau décret fixant les conditions de déclaration sur la base des propositions de comité de pilotage sera examiné prochainement par le Conseil d'État et la CNIL. Le nouveau dispositif pourra entrer en vigueur au cours du premier semestre 2001. Il permettra d'éclairer les pouvoirs publics dans l'élaboration et l'évaluation de la politique de lutte contre l'infection à VIH.

Assemblée nationale, 9 octobre 2000, n° 41 (p. 5786)

Secret et handicapés

4795 — 20 octobre 1997. — **M. Denis Jacquat** appelle l'attention de **M. le secrétaire d'Etat à la Santé** sur les propositions du Centre national des professions de santé (CNPS). Celui-ci souhaiterait que, pour la transmission des données informatiques, le secret médical soit respecté, et que la collecte ainsi que le traitement des informations saisies par les professionnels de santé soient assurés en dehors de tout monopole. Il le remercie de bien vouloir lui indiquer ses intentions en la matière.

Réponse. — Pour répondre au souci, exprimé non seulement par le Centre national des professions de santé mais également par la Commission nationale de l'informatique et des libertés, de la préservation des données médicales et du respect du secret médical en cas de transmissions informatiques, la carte de professionnel de santé (CPS et CPE), qui permet d'authentifier le professionnel, de signer les messages et de chiffrer les données personnelles et nominatives transmises par ordinateur, est distribuée à tous les professionnels de santé. Près de 200 000 cartes ont déjà été émises à la date du 15 avril 2000. ◦ ce dispositif est venue s'ajouter la mise en œuvre du réseau santé social (RSS), Intranet santé sécurisé. La loi du 4 janvier 1993 a prévu le codage et la transmission de ces informations aux organismes d'assurance maladie obligatoire, en complément des feuilles de soins. Ce codage est déjà en vigueur mais limité pour l'instant aux médicaments et aux actes de biologie médicale.

De même, les compétences reconnues aux médecins-conseils des caisses, notamment dans le cadre de la procédure d'exonération du ticket modérateur pour les patients atteints d'une affection de longue durée, impliquent une connaissance par les services du contrôle médical de la pathologie en cause. Il convient donc de relativiser la nouveauté du codage et de noter que le personnel concerné des caisses d'assurance maladie a, de longue date, su faire la preuve de sa capacité à respecter le secret médical qui s'impose à lui. Les caisses d'assurance maladie ont naturellement le monopole du traitement des feuilles de soins et il n'est pas envisageable que des données médicales nominatives soient adressées à d'autres organismes. En revanche, pour la transmission des feuilles de soins électroniques, les professionnels de santé ont le choix entre le RSS et d'autres opérateurs. Ces derniers, en mai 2000, transmettaient 35 % du nombre total des feuilles de soins électroniques.

Assemblée nationale, 17 juillet 2000, n° 29 (p. 4280)

TÉLÉCOMMUNICATIONS

Messages publicitaires

37980 — 29 novembre 1999. — **M. Léonce Deprez** appelle l'attention de **M. le secrétaire d'État à l'Industrie** sur la mise en garde de la Commission nationale informatique et libertés (CNIL) à l'égard des projets des opérateurs de téléphonie tendant à accorder des baisses de tarifs aux abonnés qui accepteraient l'interruption de leurs communications par des messages publicitaires. La CNIL souligne que la « contrepartie de ces tarifs préférentiels ne pèse pas uniquement sur celui qui y a consenti mais aussi sur ses interlocuteurs ». Il lui demande de lui préciser les perspectives de son action ministérielle s'inspirant de ces recommandations.

Réponse. — Les projets des opérateurs de téléphonie consistant à offrir une baisse des tarifs de communications téléphoniques en contrepartie de l'acceptation par l'abonné d'une interruption de ses communications par des messages publicitaires présentent un caractère inédit en France. Ils consistent en effet à utiliser des correspondances privées comme support d'annonces publicitaires. Aucun texte de caractère national ou international ne prévoit l'interdiction de telles offres. Le gouvernement sera néanmoins attentif à tout projet de cette nature qui doit respecter les règles minimales visant, d'une part, à assurer une information claire du consommateur (les opérateurs de téléphonie, comme fout professionnel de la vente, ont l'obligation d'informer les consommateurs sur les prix et conditions de vente des produits et des services qu'ils commercialisent — article L. 113-3 du code de la consommation), d'autre part, à préserver la vie privée et la tranquillité des personnes (loi « informatique et liberté », dispositions relatives à la liste orange). Comme l'a indiqué la CNIL, il convient que ce type d'offres prévoit les garanties suivantes : 1. l'abonné appelant qui a souhaité bénéficier d'une telle offre doit pouvoir, appel par appel et par un moyen technique simple (frappe d'un numéro spécial ou d'une touche particulière), choisir celles de ses communications téléphoniques qui seront interrompues par des messages publicitaires ; 2. la personne appelée doit être mise en mesure, par un moyen technique simple, de s'opposer à l'écoute de tout message publicitaire : en aucun cas un message publicitaire ne doit être délivré à la personne appelée avant qu'elle ait été informée de ce droit et du moyen technique mis à sa disposition pour l'exercer aussitôt ; 3. les personnes appelées ayant manifesté leur opposition ne doivent plus recevoir de tels appels ; lorsqu'un fichier d'opposition est mis en œuvre par l'opérateur afin d'éviter qu'une personne ne soit à nouveau importunée par une communication de cette nature, ce fichier ne doit comporter que le numéro de téléphone de la personne appelée, sans autre indication que celle qui exprime son opposition

et ne doit faire l'objet d'aucune utilisation ni d'aucune cession à des tiers, sous peine des sanctions qui répriment le détournement de finalité ; 4. les numéros de lignes des personnes appelées n'ayant pas, manifesté leur opposition à recevoir de tels appels ne doivent faire l'objet d'aucune exploitation commerciale sous quelque forme que ce soit, ni d'aucune cession à des tiers (annonceurs ou autres).

Assemblée nationale, 1er mai 2000, n° 18 (p. 2746)

TRAVAIL

Curriculum vitae

19608 — 21 octobre 1999. — M**. Dominique Braye** appelle l'attention de **Mme le Garde des Sceaux, ministre de la Justice,** sur la définition juridique du *curriculum vitae* (CV), sur son éventuel caractère de confidentialité et sur la protection juridique dont il peut bénéficier. Pour les personnes en recherche d'emploi, c'est devenu une pratique courante d'adresser aux recruteurs, que ce soit des entreprises, des administrations ou des collectivités locales, un CV qui retrace leur formation et leur expérience professionnelle, et précisant également leurs coordonnées personnelles et quelques données d'ordre privé, comme le statut marital ou le nombre d'enfants. On peut donc considérer que le CV est une fiche nominative contenant des données personnelles très détaillées qui présentent un caractère de confidentialité que son auteur souhaite préserver. Pendant longtemps, l'usage voulait que l'entreprise, l'administration ou la collectivité locale, retourne son CV au candidat non retenu. La situation actuelle du marché du travail fait que les entreprises, les administrations mais aussi les collectivités locales se trouvent aujourd'hui destinataires d'une masse considérable de CV qu'elles ne peuvent tous archiver. Cela implique en tout cas une gestion très lourde et problématique. On peut donc supposer que la plupart d'entre elles ne les conservent pas et les détruisent, au fur et à mesure. Le cas peut néanmoins se poser, en particulier lors d'un déménagement, que des dossiers de recrutement non détruits soient évacués et se retrouvent mis sur la voie publique, pour enlèvement par le service de collecte des déchets. En conséquence, il lui demande, dans un premier temps, de préciser le statut d'un CV au regard de la législation sur la protection des données personnelles. Enfin il lui demande de quoi cet abandon de documents nominatifs serait passible du point de vue du droit pénal. Il lui pose également la question du point de vue du droit civil, dans le cas où une personne dont les coordonnées personnelles se trouveraient mises sur la voie publique et à la disposition du premier passant venu peut-être malveillant, souhaiterait poursuivre l'entreprise, l'administration ou la collectivité locale responsable.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que l'applicabilité à un document des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés suppose que soient réunies les deux conditions de l'existence d'informations nominatives et de la présence d'un traitement automatisé ou d'un fichier. Sous réserve de l'appréciation par les juridictions des circonstances de l'espèce, et alors même qu'un *curriculum vitae* est un document contenant des données nominatives dont certaines présentent un caractère de confidentialité, le simple fait d'accumuler et de conserver sans les restituer à leurs auteurs des documents de cette nature, en l'absence de tout critère d'organisation et de structuration de ceux-ci, n'apparaît pas constitutif par lui seul de l'existence d'un fichier. C'est seulement dans la mesure où cette existence pourrait être préalablement établie qu'un certain nombre de droits fondamentaux énoncés par la loi susvisée du 6 janvier 1978 deviendraient applicables, en vertu de l'article 45 de celle-ci. Il en irait ainsi de l'article 29 de cette loi selon lequel « Toute

personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. ». Les articles 226-17 et 226-23 du code pénal prévoient et répriment d'une peine de cinq années d'emprisonnement et d'une amende de deux millions de francs le manquement à cette obligation. Ainsi, l'abandon sur la voie publique des documents susmentionnés pourrait-il constituer, sous réserve de l'appréciation des juges du fond, un tel manquement, toutes les précautions utiles n'ayant pas été prises pour empêcher que les données nominatives qu'ils contiennent ne soient rendues accessibles à des tiers non autorisés. En outre, en vertu des dispositions de l'article 226-24 du code pénal, une personne morale peut être déclarée responsable de l'infraction précitée. Sur un plan civil et quel que soit le statut des documents considérés au regard de la législation de protection des données, l'abandon sans protection par leur détenteur de documents présentant un caractère confidentiel à l'égard de la vie privée des personnes que ceux-ci concernent peut, sous réserve de l'appréciation par les juridictions des circonstances d'un tel abandon et des risques de divulgation auxquels il expose les intéressés, s'avérer constitutif d'une atteinte au droit de toute personne au respect de sa vie privée, édicté par l'article 9 du code civil, et être sanctionné, en conséquence, tant par des mesures susceptibles d'être ordonnées en référé par le juge afin d'empêcher ou de faire cesser une telle atteinte, que par la mise en œuvre des règles de la responsabilité civile prévues par les articles 1382 et 1383 du code civil.

Sénat, 2 avril 2000, n° 16 (p. 1459)

VIE PRIVÉE

Utilisation des fichiers d'état civil

18310 — 5 août 1999 — **M. Hubert Haenel** appelle l'attention de **M. le ministre de l'Intérieur** sur l'avis rendu par la Commission nationale de l'informatique et des libertés, le 8 avril dernier, interdisant aux maires d'utiliser les informations portées sur les registres d'état civil à l'occasion des naissances, décès et mariages, à des fins de communication personnalisée. La convivialité, l'humanité et la proximité des relations maire/administrés risquent en effet d'en pâtir. Il lui demande si une telle interdiction ne pourrait pas être limitée et ne concerner que les communications qui ont un caractère de propagande politique ou ont lieu en période pré-électorale. — ***Question transmise à M^{me} le Garde des Sceaux, ministre de la Justice.***

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la position défavorable prise par la Commission nationale de l'informatique et des libertés (CNIL) dans sa délibération n° 99-24 en date du 8 avril 1999 à l'égard de projets de fichiers destinés à permettre aux maires d'utiliser les registres de l'état civil afin d'adresser des courriers personnalisés à leurs administrés lors de naissances, mariages ou décès, est fondée sur la nécessité du respect du principe de spécification de la finalité des traitements de données à caractère personnel et qu'elle tient également compte de la mission de service public confiée par la loi aux officiers d'état civil, ainsi que de l'absence pour les personnes concernées de la possibilité d'exercer un droit d'opposition à l'endroit du traitement de leurs données dans les registres d'état civil tenus par les communes. La CNIL a rappelé dans l'avis précité le fait que le principe de finalité constituait une garantie essentielle au respect de la vie privée et de la tranquillité des personnes, tout particulièrement lorsque des fichiers publics sont en cause. Par ailleurs, il doit être

souligné que l'utilisation par les officiers d'état civil à des fins de communication personnalisée des informations portées sur les registres dont ils sont responsables n'a pas été prévue par le décret modifié n° 62-921 du 3 août 1962, dont les dispositions restrictives, prévoyant un accès limité au registre et des règles strictes de publicité des actes de l'état civil, ont été édictées dans le souci de respecter la confidentialité de la vie privée. Ces éléments conduisent à considérer que, si légitime fût-il par ailleurs, le souci de proximité des maires avec leurs administrés ne constitue pas un motif suffisant pour qu'il soit envisagé d'introduire dans les textes une dérogation importante à des principes fondamentaux de protection des personnes, même en la limitant aux communications qui n'ont pas un caractère de propagande politique ou qui n'auraient pas lieu en période préélectorale.

Sénat, 2 mars 2000, n° 9 (p. 790)

Traces informatiques

19609 — 21 octobre 1999 — **M. Dominique Braye** appelle l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur la qualification juridique de l'abandon de traces de fichiers informatiques nominatifs sur la voie publique. En effet, depuis la loi n° 78-17 du 6 janvier 1978 dite loi « Informatique et liberté », les fichiers informatiques qui contiennent des informations nominatives sont protégés et doivent être déclarés auprès de la Commission Informatique et libertés (CNIL). Le texte de cette loi est assez clair concernant la protection dont bénéficient les données électroniques nominatives, c'est-à-dire contenues sur disques durs ou disquettes. Par contre, rien n'est dit au sujet des mêmes fichiers imprimés sur papier, dont on ignore s'ils bénéficient de la même protection. La plupart du temps, les entreprises qui détiennent de tels fichiers, notamment leurs services du personnel, détruisent ces sorties papier après usage. Le cas peut néanmoins se poser, en particulier lors d'un déménagement, que des dossiers de recrutement, non détruits, et contenant ces traces papier de fichiers informatiques nominatifs, soient évacués et se retrouvent mis sur la voie publique, pour enlèvement par le service de collecte des déchets. En conséquence, il lui demande quelle protection est accordée aux traces papier de fichiers informatisés nominatifs. Enfin, il lui demande de quoi cet abandon de documents nominatifs serait passible du point de vue du droit pénal. Il lui pose également la question du point de vue du droit civil, dans le cas où une personne dont les coordonnées personnelles se trouveraient mises sur la voie publique et à la disposition du premier passant venu peut-être malveillant, souhaiterait poursuivre l'entreprise, l'administration ou la collectivité locale responsable.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que l'article 45 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a prévu l'extension d'un certain nombre des droits fondamentaux que celle-ci énonce aux fichiers non automatisés ou mécanographiques autres que ceux dont l'usage relève du strict exercice du droit à la vie privée. Il en va ainsi notamment de l'article 29 de cette loi, selon lequel : « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. » Une telle obligation de sécurité et de confidentialité, à la charge du responsable du traitement, couvre également les tirages sur supports papier correspondant aux informations nominatives incluses dans un fichier informatique ou dans tout autre traitement automatisé au sens de l'article 5 de la loi susvisée. Les articles 226-17 et 226-23 du code pénal prévoient et répriment d'une peine de cinq années d'emprisonnement et d'une

amende de deux millions de francs le manquement à cette obligation. Ainsi, l'abandon sur la voie publique des documents susmentionnés pourrait-il constituer, sous réserve de l'appréciation des juges du fond, un tel manquement, toutes les précautions utiles n'ayant pas été prises pour empêcher que les données nominatives qu'ils contiennent ne soient rendues accessibles à des tiers non autorisés. En outre, en vertu des dispositions de l'article 226-24 du code pénal, une personne morale peut être déclarée responsable de l'infraction précitée. Sur un plan civil, et quel que soit le statut des documents considérés au regard de la législation de protection des données, l'abandon sans protection par leur détenteur de documents présentant un caractère confidentiel à l'égard de la vie privée des personnes que ceux-ci concernent peut, sous réserve de l'appréciation par les juridictions des circonstances d'un tel abandon et des risques de divulgation auxquels il expose les intéressés, s'avérer constitutif d'une atteinte au droit de toute personne au respect de sa vie privée, édicté par l'article 9 du code civil, et être sanctionné, en conséquence, tant par des mesures susceptibles d'être ordonnées en référé par le juge afin d'empêcher ou de faire cesser une telle atteinte, que par la mise en œuvre des règles de la responsabilité civile prévues par les articles 1382 et 1383 du code civil.

Sénat, 20 avril 2000, n° 16 (p. 1460)

PACS

38775 — 13 décembre 1999. — **M. Bernard Accoyer** attire l'attention de **M^me^ le Garde des Sceaux, ministre de la Justice,** sur l'élaboration du décret d'application relatif à l'enregistrement des pactes civils de solidarité. Dans une édition du 28 novembre dernier, un quotidien national faisait état d'une délibération de la Commission nationale de l'informatique et des libertés (CNIL), transmise au Conseil d'Etat le 26 octobre, qui émet des réserves expresses sur l'accès aux registres. Dans la mesure où il s'agit d'un contrat opposable aux tiers et où la conclusion d'un PACS équivaut à une démarche de reconnaissance mutuelle d'une relation entre deux personnes, cette délibération de la CNIL, présidée par le « promoteur » et rapporteur de la proposition de loi devant l'Assemblée nationale, n'est pas sans poser problème. Dans sa décision du 9 novembre dernier, le Conseil constitutionnel soulignait en effet que le texte « prévoit des règles d'enregistrement des pactes civils de solidarité qui ont une double finalité, d'une part, elles visent à assurer le respect des règles d'ordre public régissant le droit des personnes, au nombre desquelles figure, en particulier, la prohibition de l'inceste et, d'autre part, elles tendent à conférer date certaine au pacte civil de solidarité pour le rendre opposable aux tiers, dont il appartient au législateur de sauvegarder les droits ; (d'autant) que l'enregistrement n'a pas pour objet de révéler les préférences sexuelles des personnes liées par le pacte ». Dans ces conditions, il lui demande de bien vouloir lui assurer que les droits des tiers seront respectés, notamment le droit des bailleurs d'accéder aux registres afin qu'ils puissent être informés en cas de transfert du bail sur une autre personne.

Réponse. — Le Garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'il appartenait au pouvoir réglementaire, selon la formule même dont use le Conseil constitutionnel dans sa décision n° 99-419 DC du 9 novembre 1999, de concilier dans le décret prévu par l'article 15 de la loi du 15 novembre 1999 relative au pacte civil de solidarité la protection des droits des tiers et le respect de la vie privée des personnes liées par celui-ci. Un tel objectif de conciliation entre deux séries de droits fondamentaux commandait une solution consistant non pas à ouvrir à tout tiers au contrat l'accès aux informations nominatives relatives au pacte civil de solidarité, mais plutôt à autoriser cet accès pour certaines catégories spécifiques de tiers, eu égard à l'intérêt légitime dont celles-ci se

prévalent. Cette interprétation a été confirmée par la Commission nationale de l'informatique et des libertés (CNIL) qui, dans sa délibération du 25 novembre 1999, a examiné, pour chacune des catégories de tiers habilitées à un accès aux registres par le projet de décret du gouvernement, si la communication des informations nominatives susmentionnées constituait une mesure ou non proportionnée, compte tenu de la nature de l'intérêt en cause ainsi que des risques d'atteinte à la vie privée. S'agissant des bailleurs de locaux, qui ne figurent pas parmi les tiers habilités par l'article 5 du décret n° 99-1090 du 21 décembre 1999, la CNIL a estimé que leur accès aux registres du pacte civil de solidarité pourrait être de nature à leur permettre d'effectuer un tri entre les candidatures à la souscription d'un bail et d'éliminer celles d'entre elles qui émanent de personnes liées par un tel pacte. L'avis de la CNIL a paru devoir à cet égard être suivi, dans la mesure où l'intérêt qui s'attache à une communication des données du bailleur ne peut être considéré comme prévalant par rapport au risque d'immixion dans la vie privée et, partant, de discrimination qui s'attacherait à cette même communication.

Assemblée nationale, 22 mai 2000, n° 21 (p. 3148)

Annexe 8

Listes d'opposition

RADIATION DES FICHIERS COMMERCIAUX

Il convient de s'adresser directement aux sociétés émettrices des *mailing* que l'on reçoit ainsi qu'aux sociétés de vente par correspondance dont on est client en leur demandant de ne pas céder ses coordonnées à des entreprises extérieures.

Il est aussi recommandé de s'adresser à :

• L'Union française du marketing direct
« Stop publicité »
60, rue la Boëtie
75008 paris

L'UFMD a mis en place un système « Stop publicité » grâce auquel il transmet des demandes de radiation à l'ensemble de ses adhérents (entreprises de vente par correspondance et de presse). Il n'intervient pas auprès des sociétés non adhérentes.

• L'agence commerciale de France Télécom dont on dépend.

Les abonnés figurant sur l'annuaire, mais qui ne souhaitent pas que les informations les concernant soient cédées par France Télécom à des entreprises menant des opérations de prospection commerciale, peuvent s'inscrire gratuitement sur la « liste orange ». De même, la « liste SAFRAN » recense les abonnés ayant demandé à ne pas recevoir de prospection par télécopie ou par télex ; à cet égard, la CNIL recommande aux opérateurs de marketing direct de ne pas procéder à des envois entre 19 heures et 8 heures.

Attention : toute commande, demande d'abonnement ou de catalogue postérieure à ces démarches peut conduire à la réinscription des coordonnées des demandeurs dans un ou des fichiers commerciaux.

OPPOSITION ◦ FIGURER DANS CERTAINS ANNUAIRES

Les abonnés figurant dans les annuaires téléphoniques édités sur support papier ou sur minitel, peuvent demander sans frais supplémentaire, à ne pas apparaître dans un annuaire téléphonique diffusé sur Internet ou dans un annuaire inversé, en s'adressant directement aux sociétés qui les diffusent.

Annexe 9

La protection des données personnelles en Europe et dans le Monde

1 — La protection des données dans l'Union européenne

Pays	Convention 108	Législation	Autorité de contrôle
Allemagne	signature 28/01/81 ratification 18/06/85 en vigueur 01/10/85	♦ Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données, modifiée par la loi fédérale de protection des données du 20 décembre 1990 et amendée par la loi du 14 septembre 1994 ♦ Transposition directive 95/46/CE : Projet de loi	Der Bundesbeauflragte **fur** den Datenschutz (autorité fédérale) Postfach 200112 53131 Bonn Web : www.datenschutz.de
Autriche	signature 28/01/81 ratification 30/03/88 en vigueur 01/07/88	♦ Loi fédérale sur la protection des données du 18 octobre 1978, amendée en 1986 ♦ Transposition directive 95/46/CE : Data protection act 2000	Direktor Buro der Datenschutzkommission nd des Datenschutzrates Bundeskanzleramt Ballhausplatz 1 1014 Vienne
Belgique	signature 07/05/82 ratification 28/05/93 en vigueur 01/09/93	♦ Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 ♦ Transposition directive 95/46/CE : Loi du 11 décembre 1998 ♦ Arrêté royal du 13 mars 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection des données personnelles	Commission de la protection de la vie Privée Porte de Hal, 5-8 Bruxelles 1060 Web : www.privacy.gov.be
Danemark	signature 28/01/81 ratification 23/10/89 en vigueur 01/02/90	♦ Loi n° 293 du 8 juin 1978 sur les registres privés et loi n' 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991 ♦ Transposition directive 95/46/CE : Loi partielle du 1er oct. 1998 et loi n° 429 du 31 mai 2000	Datatilsynet Christians Brygge 28 4 sal 1559 Copenhague Web : www.datatilsynet.dk
Espagne	signature 28/01/82 ratification 31/01/84 en vigueur 01/10/85	♦ Loi du 29 octobre 1992 réglementant le traitement automatisé de données personnelles ♦ Transposition directive 95/46/CE : Loi du 13 décembre 1999	Agencia de Protection de Datos C/Sagasta, 22 Madrid 28004 Web : www.ag-protecciondatos.es
Finlande	signature 10/04/91 ratification 02/12/91 en vigueur 01/04/92	♦ Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police ♦ Transposition directive 95/46/CE : Loi n° 523 du 10 février 1999	Le Médiateur à la protection des données Albertinkatu 25 Boîte postale 315 00181 Helsinki Web : www.tietosuoja.fi

Pays	Convention 108	Législation	Autorité de contrôle
Fronce	signature 28/01/81 ratification 24/03/83 en vigueur 01/10/85	♦ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ♦ Transposition directive 95/46/CE : Avant-projet de loi	Commission nationale de l'informatique et des libertés 21, rue Saint-Guillaume 7540 Paris cedex 07 Web : www.cnil.fr
Grèce	signature 7/02/83 ratification 11/06/95 en vigueur 01/12/95	♦ Loi n° 2472 sur la protection des personnes à l'égard du traitement des données à caractère personnel du 26 mars 1997 ♦ Transposition directive 95/46/CE : Effectuée par la loi n° 2472 du 26 mars 1997	Commission pour la protection des données 12, rue Valaoritou 10671 Athènes Web : www.dpa.gr
Irlande	signature 18/12/86 ratification 25/04/90 en vigueur 01/08/90	♦ Loi sur la protection des données du 13 juillet 1988 ♦ Transposition directive 95/46/CE : Projet de loi	Data protection commissioner **Block 4, Irish Life Center** Talbot Street — Dublin 1 Web : www.dataprivacy.ie
Italie	Signature 02/02/83 ratification 29/03/97 en vigueur 01/07/97	♦ Loi n° 675 du 31 décembre 1996 sur la protection des données personnelles, modifiée par plusieurs décrets législatifs de 1997, 1998 et 1999 ♦ Transposition directive 95/46/CE : Effectuée par la loi n' 675 du 31 décembre 1996 et des décrets législatifs ♦ Loi n°325 sur les mesures de sécurité dans le traitement des données personnelles du 3 novembre 2000	Garante per la protezione dei dati Personali Largo del Teafro Valle 6 00186 Rome Web : www.garanteprivacy.it
Luxembourg	Signature 28/01/81 ratification 10/02/88 en vigueur 01/06/88	♦ Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, amendée en 1992. ♦ Transposition directive 95/46/CE : Projet de loi	Commission consultative à la protection des données 16 boulevard Royal 2934 Luxembourg
Pays-Bas	signature 21/01/88 ratification 24/08/93 en vigueur 01/12/93	♦ Loi du 28 décembre 1988 sur la protection des données, complétée par une loi du 21 juin 1990 sur les fichiers de police ♦ Transposition directive 95/46/CE : Loi du 6 juillet 2000	Registratiekumer Prins Clauslaan 20 Postbus 93374 -2509 AJ's-Gravenhage Web : www.registertiekamer.nl
Portugal	signature 4/05/81 ratification 02/09/93 en vigueur 01/01/94	♦ Loi n° 10/91 du 29 avril 1991 sur la protection des données à caractère personnel face à l'informatique, amendée par une loi du 29 août 1994 ♦ Transposition directive 95/46/CE : Loi n° 67/98 du 26 octobre 1998 sur la protection des données personnelles	Comissào Nacional de Potecçào de Dados Informatizados **148, rue de Sao** Bento 1200-82 Lisbonne Web : www.cndp.pt

Pays	Convention 108	Législation	Autorité de contrôle
Royaume-uni	signature 4/05/81 **ratification 26/08/87** en vigueur 01/12/87	♦ Loi sur la protection des données du 12 juillet 1988. ♦ Transposition directive 95/46/CE : Loi du 16 juillet 1998 sur la protection des données. ♦ Loi sur l'accès à l'information du 30 novembre 2000	The office of information Commissioner Wycliffe House — Water Lane Wilmslow — Cheshire SK9 5AF United Kingdorn Web : www.dataprotection.gov.uk
Suède	signature 28/01/81 ratification 29/09/82 en vigueur 01/10/85	♦ Loi du 11 mai 1973 sur la protection des données ♦ Transposition directive 95/46/CE : Loi n° 204 du 24 octobre 1998 sur la protection des données.	Datainspektionen Box 8114 104 20 Stockholm Web : www.datainspektionen.se

2 — La protection des données hors de l'Union européenne

Pays	Convention 108	Législation	Autorités de contrôle / Contacts
Albanie		♦ Loi n° 8517 sur la protection des données personnelles - 1999	
Afrique du Sud		♦ Promotion of access to information act -2000	
Argentine		♦ Loi n' 25 326 sur la protection des données personnelles - 2 novembre 2000	
Australie		♦ Loi fédérale sur la vie privée - 1988 (Secteur public), amendement sur la protection des données dans le secteur privé - 6 décembre 2000	Federal Privacy Commission GPO Box 5218 - Sydney NSW 1024 Web : www.privacy.gov.au
Bulgarie	signature 02/06/98		
Canada		♦ Loi fédérale sur la protection des renseignements personnels – 1982 ♦ Loi fédérale sur la protection des renseignements personnels et les documents électroniques - 2000	Federal privacy commission Tower B, 3rd Floor, 112 Kent Street - Otawa, Ontario K1A 1H3 Web : www.privcom.gc.ca
Chypre	signature 27/07/86		
Corée (sud)		♦ Loi sur la protection des données personnelles - 1994	
Estonie	signature 24/01/00	♦ Loi sur la protection des données personnelles - 1997	Andmekaitse Inspektsion Pikk 61 EE 10133 Tallinn Web : www.dp.gov.ee

Pays	Convention 108	Législation	Autorités de contrôle / Contacts
États-Unis		♦ Loi sur la protection des libertés individuelles – 1974 ♦ Diverses lois sectorielles relatives à la protection des données Ex : **The** video privacy protection Act – 1988 Electronic Freedom of Information Act – 1996 Children's Online Privacy Protection	Nat. Telecommunications & Information Adm. US Depart, of commerce — room 4713 14th constitution avenue NW USA Washington DC 20230
Guernsey	par extension en vigueur 01/12/87	♦ Loi sur la protection des données –1986 ♦ Projet de loi modificatif - 26 juillet 2000	The data protection **officer** PO Box 43 **La Charroterie** St Peter Port Guernsey G71 1FH Web : www.dpcommission.gov.gg
Hong-Kong		♦ Loi sur la protection des données -1990 ♦ Ordonnance sur la protection des données - 1995	Privacy commission for personal data Unit 2001, 20/F - Office Tower Convention Plaza -1 Harbour Road Wan Chai — Hong Kong Web : www.pco.org.hk
Hongrie	Signature 13/05/93 ratification 08/10/97 en vigueur 01/02/98	♦ Loi sur la protection des données personnelles et la communication de données publiques -1992	Parliamentary commissioner for data protection and freedom of information **Tükry u 3 H - 1054 Budapest** **Web : www.obh.hu**
Ile de man	par extension en vigueur 21/01/93	♦ Loi sur la protection des données -1986	Data protection registrar PO Box 69 Douglas **IM99 1EQ — Ile de Man**
Inde		♦ The information technology act -9 juin 2000	
Islande	Signature 27/09/82 ratification 25/03/91 en vigueur 01/07/91	♦ Loi n° 63-1981 relative à l'enregistrement de données personnelles -1981 (amendée en 1989) ♦ Loi n° 77 on Protection of individuals with regard ta the processing of personal data 23 mai 2000	Personuvernd Rauôarasfigur 10 105 Reykjavik Iceland Web : www.personuvernd.is
Israël		♦ Loi n° 5741 sur la protection de la vie privée -1981 (amendée en 1985 et 1996) ♦ Loi n° 5746 sur la protection des données dans l'Administration 1986	Registrar of data bases **Hashlocha 2 Yad Eliahu** PO Box 9288 Tel Aviv — Israël
Japon		♦ Loi sur la protection des données personnelles informatisées dans le secteur public - 1988	Governement information Systems planning division 1-1 Kasumigaseki 3 — Chiyoda-ku Tokyo 100 Japon
Jersey	par extension en vigueur 01/12/87	♦ Loi sur la protection des données -1987	Data protection registry States Greffe Westway Chambers Don Street **St Helier JE 24TR**
Lettonie	signature 31/10/00	♦ Loi sur la protection des données -1998	

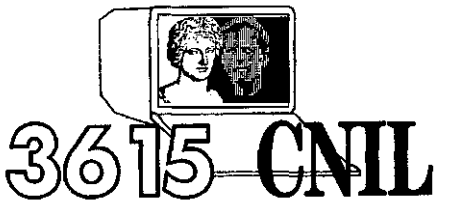
Pays	Convention 108	Législation	Autorités de contrôle / Contacts
Lituanie	signature 11/02/00	♦ Loi sur la protection des données personnelles -1996	State Dota Protection Inspectorate Gedimino av. 27/2 Vilnius Lithuania Web : www.is.lt/dsinsp
Moldavie	signature 04/05/98 .		
Monaco		♦ Loi n° 1165 relative aux traitements d'informations nominatives - 1993	Commission de contrôle des informations nominatives Ministère d'État Place de la Visitation 98000 Monaco
Norvège	signature 13/03/81 ratification 20/02/84 en vigueur 01/10/85	♦ Loi sur les registres de données personnelles –1978 ♦ Loi sur la protection des données personnelles - 14 avril	Datatilsynef Postboks 8177 Dep 0034 Oslo 1 Web : www.datatilsynet.no
Nouvelle -Zélande		♦ Loi sur l'information du secteur public – 17 décembre 1982 ♦ Loi sur la vie privée -	Privacy commission PO Box 466 Auckland Web : www.privacy.org.nz
Paraguay		♦ Loi sur la protection des données - 28 décembre 2000	
Pologne	signature 21/04/99	♦ Loi sur la protection des données personnelles - 1997	Biuro Geneeralnego Inspektora Pl. PowstancowWarszawy 1 00-030 Warszawa
Républiq ue de St-Marin		♦ Loi relative à la protection des données personnelles - 1983 (amendée en 1995)	
Républi que Tchèque	signatur e 08/09/ 00	♦ Loi relative à la protection des données personnelles des systèmes informatisés –1992 ♦ Loi n° 101/2000 sur la protection des données	Office for personal data protection Havelkova 22, CZ-130 00 Praha 3 Czech Republic web : www.uoou.cz
Républiqu e de Macédoin		♦ Loi sur la protection des données personnelles - 1994	
Roumanie	Signature **18/03/97**	♦ Loi créant la Commission nationale pour l'informatique - 1990	Commission nationale de l'informatique 1, place de la victoire R-71 201 Bucarest 1
Russie		♦ Loi fédérale sur l'information, l'informatisation et la protection des	
Slovaquie	signature 14/04/00 ratification 13/09/00 en vigueur 01/01/01	♦ Loi relative à la protection des données personnelles des systèmes informatisés -**1998**	Statistical Office of Slovokia Dùbravska 3 SK-84221 Bratislava

Pays	Convention 108	Législation	Autorités de contrôle / Contacts
Slovénie	signature 23/11/93 ratification 23/11/93 en vigueur 01/09/94	♦ Loi n° 210-01/89-3 sur la protection des données - 1999	**Mînistry** of justice Zupancicceva 3 SLO - 1000 **Lubjana**
Suisse	signature 02/10/97 ratification 02/10/97 en vigueur 01/02/98	♦ Loi fédérale sur la protection des données - 1992	Commissaire à la protection des données Monbijoustrasse 5 3003 Berne Web : www.edsb.ch
Taiwan		♦ Loi sur la protection des données -1995	The **ministry** of justice 130, Sec 1, Chung Ching South Road Taipei 100 —Taiwan
Thailande		♦ Loi sur la protection des données dans le secteur public - 1998	Officiai Information Commission's Office The prime Minister's Office Governement House Bangkok 10300 Thailand
Turquie	signature 28/01/81		

Communauté européenne	Directive européenne n° 95/46/CE relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données -24 octobre 1995	Commission européenne DG XV 200 rue de la Loi - Bruxelles B -1049 Belgique Web : http : //europa.eu.int/comm/dg15/fr /media/index.htm
Conseil de l'Europe	Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel - 28 janvier 1981	Conseil de l'Europe Direction des affaires juridiques Section protection des données 67075 Strasbourg — France Web : www.cœ .fr/dataprotection
OCDE	Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel - 23 septembre 1980	OCDE 2, rue André Pascal 75775 Paris cedex 16 Web : www.cœ cd.org/index-fr.htm
ONU	Lignes directives pour la réglementation des fichiers informatisés de données à caractère personnel - 1989	Web : www.unhchr/french/html/intlinsLfr.htm

Commission nationale
de l'informatique et des libertés
21, rue Saint-Guillaume
75340 Paris Cedex 07
Tél. 01 53 73 22 22
Télécopie : 01 53 73 22 00

POUR PLUS D'INFORMATIONS :



Site Internet : http ://www.cnil.fr

Impression : EUROPE MEDIA DUPLICATION S.A.
53110 lassay-les-Châteaux
N° 8559 - Dépôt légal : juin 2001

Le 21e rapport d'activité de la Commission Nationale de l'Informatique et des Libertés illustre la très grande variété des champs d'intervention de la CNIL et l'importance des sujets que cette autorité indépendante est amenée à traiter.

Des fichiers d'attribution des logements sociaux au registre épidémiologique de lutte contre le VIH sans oublier le Système de Traitement des Infractions Constatées (STIC) du ministère de l'Intérieur, la CNIL doit arbitrer entre des intérêts contradictoires et évoque, pour chacun de ces sujets, les termes du débat autour d'exposés faciles d'accès pour le lecteur non averti mais précis et complets pour les spécialistes.

Le développement des nouvelles technologies et leurs incidences sur notre vie privée sont également très largement traités, qu'il s'agisse de la cybersurveillance des salariés dans l'entreprise, des dossiers médicaux sur internet, du contrôle d'accès par biométrie ou de la sécurisation des cartes bancaires.

Enfin, l'avis de la CNIL sur le projet de loi de la société de l'information ainsi que la réforme attendue de la loi du 6 janvier 1978 font l'objet de développements inédits qui donnent un éclairage précieux sur ces deux très importants chantiers législatifs, au moment de « la mondialisation de la protection des données » à laquelle le présent rapport consacre sa dernière partie.

Prix : 20€ / 131,19F
La Documentation française
29-31, quai Voltaire
75344 Paris Cedex 07
Téléphone : 01 40 15 70 00
Télécopie : 01 40 15 72 30
www.ladocfrancaise.gouv.fr
Imprimé en France
ISBN : 2-11-004861-1
DF : 5 6047-2