COMMISSION
NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

20e rapport d'activité 1999

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

ISBN 2-11-004614-7

Sommaire

Un fichier épidémiologique de suivi de la séropositivité au sida, le fichier national d'empreintes génétiques des personnes condamnées pour infraction sexuelle, une loi autorisant l'administration fiscale à utiliser le NIR, l'informatisation des registres d'inscription des pactes civils de solidarité, le recensement général de la population, et Internet toujours, moyen désormais le plus puissant de collecter des données personnelles à l'échelle mondiale : la CNIL a été tout au long de cette année 99 au cœur de l'actualité.

Alors, ce XX^{e} rapport d'activité serait-il le journal intime de « Big Brother » ?

Nullement, car au-delà de l'action de la CNIL, jamais sans doute nos concitoyens n'ont manifesté avec autant de force, et parfois de passion, leur attachement aux droits qui leurs sont reconnus par la loi du 6 janvier 1978 et leur souci de transparence, tant à l'égard de l'Etat, de ses procédures, de ses fichiers, qu'à l'égard des entreprises avec lesquelles ils sont en contact dans leur vie quotidienne. Cette vigilance est un beau signe de vitalité et un élément qui concourt à l'équilibre entre *informatique* et *libertés*.

C'est cet équilibre que le législateur de 1978 a recherché en édictant des principes simples et clairs qui constituent un utile viatique à l'heure de la société de l'information. La CNIL l'a déjà souligné : la constitution d'un fichier résultait jadis d'une volonté. Nous étions fichés parce que quelqu'un souhaitait nous ficher. Aujourd'hui, nous pouvons aussi être « fichés » du seul fait de la technologie qui produit des traces sans que nous en ayons toujours pleinement conscience. Ces traces constituent autant de gisements de données qui touchent à notre vie privée et qui peuvent être exploitées, détournées, portées à la connaissance de tiers.

Jamais sans doute les principes établis par la loi du 6 janvier 1978 n'ont eu une telle actualité. A l'heure des réseaux et du « tout numérique », ces principes sont autant de sauvegardes : principe de finalité, contrôle de la pertinence des données collectées, confidentialité des informations nominatives, droit d'accès et de rectification, droit d'opposition, droit à l'oubli enfin.

Jamais, en tout cas, ces principes n'ont eu une telle force. Désormais communs à tous les Etats membres de l'Union européenne, ils sont en voie d'être consacrés au plan mondial. La discussion bilatérale en cours entre l'Europe et les Etats-Unis sur les flux transfrontières de données en est l'illustration. Certains avaient pu redouter que la législation française ne résiste ni à la globalisation des échanges ni à l'internationalisation de la société de l'information. Force est pourtant de constater que l'expérience française de la protection des données personnelles a convaincu l'Europe, et qu'Internet devient un puissant instrument de diffusion de la culture « informatique et libertés » dans le monde.

Il nous reste à actualiser la loi du 6 janvier 1978 puisque la directive européenne du 24 octobre 1995 nous y invite. Le moment est évidemment venu. Il nous appartient collectivement de veiller à renforcer la confiance, tous les acteurs privés ou publics doivent s'en convaincre. Les responsables de traitements devraient devenir des relais « informatique et libertés » et participer ainsi à la protection des données personnelles désormais conçue, non plus seulement comme une obligation, mais comme la condition indispensable d'une relation confiante avec nos concitoyens.

Michel Gentot

AU CŒUR DE L'ACTUALITÉ

I. UNE FORTE ACTIVITÉ

A. 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 à des auditions. L'année 99 n'a pas fait exception à cette règle.

Ainsi, avant de se prononcer sur la délicate question du fichier des déclarations obligatoires de séropositivité au VIH, la Commission a souhaité consulter des associations de défense des malades atteints du sida, la Ligue des droits de l'Homme et le Conseil national de l'ordre des médecins. Elle a également tenu à rencontrer des médecins inspecteurs des directions départementales de l'action sanitaire et sociale (cf infra chapitre 5).

De même, l'examen du fichier national automatisé des empreintes génétiques, créé en vue de faciliter l'identification et la recherche des auteurs d'infractions sexuelles, a conduit la CNIL à se rendre au laboratoire médico-légal de Bordeaux, du laboratoire de génétique moléculaire du centre hospitalier régional et universitaire de Nantes, au laboratoire de police scientifique de Paris ainsi qu'à l'Institut de recherche criminelle de la gendarmerie nationale (cf infra dans ce chapitre, point II. A).

Enfin, dans le cadre d'une étude d'ensemble sur le publipostage électronique et le « spam », la CNIL a souhaité consulter l'ensemble des acteurs concernés et des associations représentatives, des fournisseurs d'accès à internet, des gestionnaires de listes de diffusion, des organismes de normalisation et des professionnels du commerce et de l'édition de contenus électroniques ou de la vente à distance (cf infra chapitre 3).

Par ailleurs, la CNIL a procédé en 1999 à plusieurs auditions en séance plénière :
— sur l'utilisation du NIR par les administrations fiscales, la CNIL a entendu le ministre délégué au Budget, ainsi que le directeur général des impôts,
— sur la procédure rénovée du recensement général de la population, la Commission a procédé à l'audition du directeur général de l'INSEE.

A ces missions d'information et de concertation, se sont ajoutées plus d'une trentaine de missions de contrôle ou de vérification sur place, au titre du contrôle a posteriori du fonctionnement de fichiers des données personnelles.

Ces missions de contrôle a posteriori étant appelées à se développer, notamment dans la perspective de la transposition de la directive européenne du 24 octobre 1995, la CNIL a souhaité renforcer le caractère contradictoire de la procédure d'investigation, de contrôle ou de vérification sur place.

Le règlement intérieur de la Commission précisait déjà que toute mission de contrôle devrait faire l'objet d'un rapport, ce rapport étant communiqué à la personne concernée qui dispose d'un délai de 15 jours pour faire connaître ses observations. La personne concernée disposait en outre du droit d'être entendue par la Commission, assistée ou non d'un conseil.

En pratique, cette dernière faculté a peu été utilisée, ce qui est regrettable.

Aussi, est-il désormais précisé dans le règlement intérieur de la Commission que le rapport communiqué à la personne ou à l'organisme en cause doit comporter les conclusions du rapporteur, c'est-à-dire les propositions que le commissaire-rapporteur soumettra à l'examen de la séance plénière. Lorsque les propositions du rapporteur tendront à voir délivrer un avertissement ou dénoncer des faits au Parquet, l'audition sera de droit. Dans les autres cas, il reviendra au bureau de la Commission de décider, eu égard aux propositions faites par le rapporteur, si une audition est ou non utile.

Il convient cependant de souligner que jusqu'à présent, aucune demande d'audition n'a été refusée par la Commission.

Délibération n° 99-043 du 9 septembre 1999 portant modification de l'article 57 du règlement intérieur de la Commission

La Commission nationale de l'informatique et des libertés,

Vu la Convention 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, pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu la délibération n° 87-25 du 10 février 1987 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés,

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

Considérant qu'il y a lieu de renforcer le caractère contradictoire de la procédure relative aux missions d'investigation, de contrôle ou de vérification sur place,

Décide :

L'article 57 du règlement intérieur de la Commission est ainsi rédigé :

« La mission fait l'objet d'un rapport signé par le membre ou l'agent de la Commission qui y a procédé. Ce rapport comporte le compte rendu de mission et les conclusions du rapporteur. Il est communiqué à la personne concernée qui est informée qu'elle dispose d'un délai de 15 jours à compter de la réception du rapport pour faire connaître ses observations et qu'elle peut demander à être entendue, assistée ou non d'un conseil, par la Commission. Cette audition est de droit lorsque le rapport de mission conclut à un avertissement ou une dénonciation au Parquet. Dans les autres cas, le bureau de la Commission apprécie la suite à donner à la demande d'audition qui est présentée. »

B. 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 des saisines sur les cinq dernières années

Nature des saisines	1995	1996	1997	1998	**1999**	Variation 1998/1999
Plaintes	1 636	2 028	2 348	2 671	**3 508**	+ 31,33 %
Demandes de conseil	985	1 008	821	1 115	**1 061**	- 4,84 %
Demandes de radiation des fichiers commerciaux	263	277	263	204	**186**	- 8,82 %
Demandes de droit d'accès indirect	243	320	385	401	**671**	+ 67,33 %
Demandes d'information générale	365	347	480	477	396	- 16,98 %
Demandes d'extraits du fichier des fichiers	122	170	155	154	**133**	- 13,63 %
Total	**3 614**	**4 150**	**4452**	**5 022**	**5 955**	+ 18,57 %

Les plaintes ont plus que doublé de 1995 à 1999. Le nombre de demandes d'accès à des fichiers de police ou de défense a presque triplé dans le même temps (cf infra dans ce chapitre).

Le nombre total de saisines continue d'augmenter (+18,5 % d'une année sur l'autre). Les plaintes, en particulier, enregistrent une progression de 31,33 % et les demandes d'exercice du droit d'accès indirect aux fichiers de police et de sécurité progressent dans une proportion inédite (+67,33 %).

Les demandes de conseil

Depuis 1978, la CNIL a reçu près de 10 000 demandes de conseil, dont 1061 pour l'année 1999. Les secteurs d'activité qui ont suscité en 1999 le nombre le plus important de demandes de conseil concernent, par ordre décroissant, la santé, le travail, la fiscalité, les collectivités locales, le commerce et tout particulièrement le commerce électronique.

Les plaintes

Depuis 20 ans, la CNIL a reçu près de 33 000 plaintes, dont 3 508 pour 1999. Les secteurs d'activité qui ont suscité le nombre le plus important de plaintes sont, par ordre décroissant, la prospection commerciale, la banque, le travail, les statistiques, ce dernier élément trouvant son explication dans les opérations de recensement général de la population.

L'objet le plus fréquent des plaintes concerne l'exercice des droits, et tout particulièrement du droit d'opposition à faire l'objet de prospection commerciale.

Les avertissements et dénonciations au parquet

L'instruction des plaintes conduit parfois la CNIL à délivrer un avertissement ou à dénoncer des faits au Parquets, conformément à l'article 21 alinéa 4 de la loi du 6 janvier 1978. En 1999, la CNIL n'a pas délivré d'avertissement mais a transmis deux affaires au Parquet.

Depuis sa création en 1978, la CNIL a délivré 47 avertissements. Les avertissements constituent des mesures qui font grief et qui sont donc susceptibles de recours devant le Conseil d'Etat (cf arrêt CE 30 juillet 1997, 18e rapport d'activité, p. 59). Le Conseil d'Etat a statué en 1999 sur deux recours pour excès de pouvoir formés contre des avertissements délivrés par la CNIL au cours des années précédentes.

Dans un arrêt du 14 juin 1999, le Conseil d'Etat a rejeté le recours formé par une société contre un avertissement qui lui avait été délivré par la CNIL le 12 mai 1998 en raison du refus qu'elle avait opposé à la demande de droit d'accès présentée par un visiteur médical souhaitant disposer, dans le cadre d'un conflit prud'hommal l'opposant à son employeur, de la liste des visites qu'il avait effectuées auprès de médecins (cf 19e rapport d'activité, p. 52). Outre le fait qu'il confirme le bien-fondé de la délibération de la CNIL, cet arrêt présente l'intérêt de préciser que

le titulaire du droit d'accès pouvait, dans le cas d'espèce, s'adresser aussi bien à la société qui l'employait qu'à la société à laquelle la mise en œuvre du traitement informatique avait été confié en vertu d'un contrat de prestation de service, sans que, dans cette dernière hypothèse, la clause de confidentialité figurant dans la convention entre les deux sociétés puisse être opposée au demandeur.

Dans un arrêt du 3 décembre 1999, le Conseil d'Etat a rejeté le recours formé contre un avertissement qui avait été délivré à un organisme bancaire le 7 avril 1998 en raison du caractère excessif et attentatoire à la vie privée de certaines informations figurant dans la zone « bloc-note » du fichier de clients. Le Conseil d'Etat a confirmé le bien-fondé de l'avertissement. Cet arrêt présente en outre l'intérêt de préciser que les modalités d'organisation du principe du contradictoire devant la CNIL n'encourent aucun grief et que, les avertissements délivrés par la CNIL n'émanant pas d'un tribunal au sens de l'article 6-1 de la convention européenne des droits de l'Homme et des libertés fondamentales, la participation des commissaires rapporteurs au débat et au vote ne constitue une méconnaissance ni du principe d'impartialité, ni des droits de la défense.

S'agissant des dénonciations, la CNIL a dénoncé au Parquet en 1999 deux organismes pour des faits graves. Cela porte à 16 le nombre de dénonciations au Parquet émises par la CNIL en 20 ans. Il convient de reconnaître que la CNIL a peu recouru à cette procédure, marquant ainsi sa préférence pour le dialogue et la concertation. Cette manière de faire est cependant parfois critiquée. Ainsi, un requérant qui avait saisi la CNIL du défaut d'informations des usagers lors de la mise en œuvre par une bibliothèque municipale d'un fichier informatique de gestion des prêts de livres a saisi la Conseil d'Etat en faisant grief à la CNIL de n'avoir pas dénoncé les faits au Parquet (cf. annexe 7). Dans un arrêt n° 196306 du 27 octobre 1999, le Conseil d'Etat a jugé que la CNIL n'était tenue de dénoncer des faits au Parquet qu'à la double condition que « ces faits lui paraissent suffisamment établis » et qu'elle « estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application ». Il résulte clairement de cet arrêt que la CNIL dispose, dans les limites précisées par le Conseil d'Etat et sous son contrôle, du pouvoir d'apprécier l'opportunité de dénoncer des faits au Parquet. Il reste que, quelle que soit la décision de la CNIL, dont le requérant est systématiquement tenu informé, toute personne peut saisir directement le Parquet d'une infraction dont elle aurait à se plaindre, la CNIL devant d'ailleurs se tenir à la disposition des autorités judiciaires pour répondre à toute demande d'avis ou de conseil que la juridiction saisie d'un contentieux touchant à la loi du 6 janvier 1978 pourrait lui présenter.

Les scouts d'Europe

La CNIL a dénoncé au parquet la divulgation d'un annuaire local des chefs et cheftaines scouts d'Europe et son utilisation par diverses publications liées à des mouvements d'extrême droite.

Saisie par les parents d'un garçon mineur, membre des scouts d'Europe, qui avait reçu à son domicile un catalogue de vente par correspondance édité par la Société d'études et de relations publiques (SERP) et comportant notamment des livres

et disques évoquant la période nazie, ainsi qu'un exemplaire du journal « Français d'abord-le magazine de Jean-Marie Le Pen », la CNIL a effectué des missions de contrôle auprès du centre national de l'association des « Guides et scouts d'Europe » et de la SERP. La CNIL a pu ainsi établir qu'un annuaire des chefs et cheftaines des scouts d'Europe de la région Provence avait été irrégulièrement divulgué et que les coordonnées du fils du plaignant qui figuraient dans cet annuaire local, avec une faute d'orthographe dans le libellé de l'adresse, avaient été utilisées à des fins de prospection commerciale et politique par la SERP, d'une part, le journal « Français d'abord », d'autre part. La CNIL n'a pu en revanche procéder à la mission de contrôle qu'elle avait décidé d'accomplir auprès du journal « Français d'abord », dont seule la boîte postale est connue, les responsables de cette publication ayant refusé par deux fois de lui communiquer le lieu où se trouvait le fichier des abonnés.

Par la suite, la Commission a été saisie d'une nouvelle plainte émanant des parents d'un autre chef scout de Provence qui avait également reçu, outre le catalogue de la SERP et un exemplaire du journal « Français d'abord », une invitation de la fédération Front national du Var à un dîner-débat en présence de M. Jean-Marie Le Pen.

Compte tenu de la gravité des faits et du nombre de jeunes scouts dont les coordonnées figuraient sur l'annuaire divulgué, la CNIL, par une délibération n° 99-017 du 25 mars 1999, a décidé de dénoncer :
— X pour n'avoir pas pris de précautions suffisantes pour empêcher que ne soient communiquées à des tiers qui n'ont pas à en connaître tout ou partie des informations nominatives, présentées sous forme de listes informatisées, se rapportant à des chefs et cheftaines des scouts d'Europe de Provence (article 226-17 du code pénal),
— la SERP et le journal « Français d'abord » pour avoir utilisé, à l'insu de la personne concernée et de son représentant légal, des informations nominatives la concernant sous forme d'étiquettes adresses issues d'un traitement automatisé d'informations nominatives (article 226-18 du code pénal),
— le journal « Français d'abord » pour entrave à l'action de la commission (article 43 de la loi du 6 janvier 1978).

La CNIL a transmis sa délibération au parquet de Nanterre, déjà saisi de faits connexes par l'association nationale des guides et scouts d'Europe.

A la date de rédaction du présent rapport, l'instruction judiciaire ouverte sur ces faits était toujours en cours.

Délibération n° 99-017 du 25 mars 1999 relative aux suites à donner aux missions de contrôle auprès de l'association des guides et scouts d'Europe, de la société SERP, du journal « Français d'abord-le magazine de Jean-Marie Le Pen » et des légionnaires du Christ et portant dénonciation au parquet

La Commission nationale de l'informatique et des libertés,

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

Vu la 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 délibérations de la Commission n° 98-102, 98-103, 98-104 et 98-105 du 22 décembre 1998 décidant des missions de contrôle auprès de la SERP, des « Légionnaires du Christ », du journal « Français d'abord » et de l'association des guides et scouts d'Europe ;

Vu les comptes rendus de mission adressés l'un le 8 février 1999 à la SERP, l'autre le 17 février à l'association des guides et scouts d'Europe ;

Vu les observations en réponse du Président de l'association des guides et scouts d'Europe en date du 4 mars 1999 ;

Vu les courriers adressés par la CNIL au journal « Français d'abord » par lettres recommandées avec accusé de réception les 6 janvier et 2 février 1999 ;

Vu le courrier adressé à la Commission par les « Légionnaires du Christ » le 19 janvier 1999 invoquant les dispositions de l'article 31 alinéa 2 de la loi au bénéfice du groupement ;

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

Considérant qu'un garçon mineur, membre de l'association des guides et scouts d'Europe, a reçu à son domicile, d'une part, un catalogue de vente par correspondance diffusé par la société d'études et de relations publiques (SERP) proposant divers articles (artisanat, bijoux) et œuvres (vidéo, livres, disques) dont certains évoquent la période nazie, d'autre part, un exemplaire du journal « Français d'abord, le magazine de Jean-Marie Le Pen », enfin un courrier émanant d'un groupement dénommé « Légionnaires du Christ » ; que ces envois, rapprochés dans le temps, ont appelé l'attention du père du mineur concerné qui a saisi la CNIL de ces faits en novembre 1998 afin de connaître l'origine des informations qui avaient été utilisées pour procéder à ces envois ;

Considérant que la Commission a, par délibération du 22 décembre 1998, décidé de procéder à plusieurs missions de contrôle sur place auprès des organismes concernés ainsi qu'auprès de l'association des guides et scouts d'Europe ;

Considérant qu'il résulte des missions de contrôle effectuées auprès du centre national de l'association des guides et scouts d'Europe et de la société SERP, éditrice du catalogue reçu par le garçon, que les informations ayant permis de solliciter le fils du plaignant, Philippe, trouvent leur origine dans un annuaire local des chefs et cheftaines scouts établi dans la région Provence à l'initiative de responsables locaux de l'association des guides et scouts d'Europe ; que l'association des guides et scouts d'Europe a indiqué que cet annuaire local avait fait l'objet d'une divulgation ; que les dires de cette association sont corroborés par le fait qu'une faute d'orthographe altérant l'adresse de l'intéressé, telle qu'elle figure dans cet annuaire local, se retrouve sur les étiquettes-adresse, que le plaignant a communiquées à la Commission, des courriers qui ont été adressés au jeune garçon par la SERP et le journal « Français d'abord » ;

Considérant en effet qu'il résulte des actes d'instruction accomplis par la CNIL que le centre national des guides et scouts d'Europe envoie à chaque chef de groupe la liste nominatives des scouts placés sous sa responsabilité ;

qu'en outre, le centre national envoie, sur leur demande, aux chefs de district ou aux commissaires de Province, rangs hiérarchiques propres à cette organisation, la liste nominative des membres de l'encadrement (chefs et cheftaines) qui sont placés sous leur autorité ; qu'en outre, les chefs de district sont destinataires, chacun pour ce qui le concerne, des coordonnées des chefs de patrouille libre, c'est-à-dire de petits groupes locaux ne comportant pas un nombre suffisant de scouts pour constituer des unités à part entière ; que le nom et l'adresse du jeune Philippe, chef de patrouille libre, figuraient sur les listes ainsi communiquées aux responsables de la région Provence ;

Considérant que la Commission a pu établir que les informations utilisées par la SERP, d'une part, par le journal « Français d'abord », d'autre part, ne provenaient pas d'une divulgation qui aurait été commise à partir des listes communiquées par le centre national de l'association des guides et scouts d'Europe aux responsables locaux dans la mesure où le fichier national des guides et scouts d'Europe duquel étaient extraites ces listes ne comporte pas de faute d'orthographe dans le libellé de l'adresse du jeune Philippe ; que les courriers qui ont été adressés à Philippe par la SERP et par le journal « Français d'abord » n'ont pu l'être qu'à la suite d'une divulgation des informations que comportait l'annuaire local des chefs scouts de Provence, comme l'atteste la faute d'orthographe qui se retrouve sur les courriers litigieux reçus ;

Considérant, dès lors, qu'un annuaire des chefs et cheftaines scouts de Provence a été divulgué en tout ou partie et en violation des dispositions de la loi du 6 janvier 1978 à des organismes qui n'avaient pas à en connaître ; qu'ainsi, l'infraction prévue par l'article 226-17 du code pénal paraît établie, sans qu'il soit possible pour la CNIL, en l'état des pouvoirs dont elle dispose, d'identifier le responsable — personne physique ou personne morale — du fichier, automatisé ou non, des chefs et cheftaines scouts de Provence auquel incombait l'obligation de prendre toutes précautions utiles afin d'empêcher que les informations nominatives ne soient communiquées à des tiers non autorisés ;

Considérant que la Commission a pris note des déclarations du Président de l'association des guides et scouts d'Europe selon lesquelles l'annuaire de Provence aurait été irrégulièrement transmis à une société commerciale dénommée DEFI qui l'aurait à son tour utilisé pour son propre compte afin d'adresser un catalogue intitulé « Durandal » à l'ensemble des personnes figurant sur l'annuaire ; que plainte a été déposée sur ces faits par l'association des guides et scouts d'Europe auprès du Parquet de Nanterre ;

Considérant que la Commission prend acte qu'à la suite de cette divulgation l'association des guides et scouts d'Europe a pris des précautions nouvelles s'agissant de la diffusion de l'annuaire des chefs et cheftaines de Provence 1998/99 ; mais considérant que ces mesures, qui ne valent que pour l'avenir, ne sauraient ni retirer à la divulgation précédemment commise son caractère frauduleux, ni aux faits leur gravité ;

Considérant de surcroît que le fichier divulgué, qui comporte près de 300 noms, peut encore à ce jour être utilisé par des personnes ou organismes qui n'ont pas à en connaître, comme semble l'attester la plainte déposée le 19 janvier 1999 auprès de la CNIL par le parent d'un autre chef scout de Provence mineur inquiet que son fils ait reçu, outre le catalogue de la SERP et un exemplaire du journal « Français d'abord », le catalogue Durandal ainsi

qu'une invitation de la fédération Front National du Var à un dîner-débat en présence de M. Jean-Marie Le Pen ;

Considérant que les investigations entreprises établissent que les informations utilisées par l'association des « Légionnaires du Christ » ne proviennent pas de l'annuaire local des chefs et cheftaines scouts de Provence ; qu'en effet, la Commission a pu constater que la faute d'orthographe figurant sur l'annuaire local ne se retrouve pas sur l'étiquette-adresse de l'envoi effectué par les « Légionnaires du Christ » au jeune Philippe, étiquette qui fait d'ailleurs mention d'une adresse plus complète que celle qui figure dans cet annuaire, ainsi que de l'adresse de l'intéressé telle qu'elle est enregistrée dans le fichier national des scouts d'Europe ; que le groupement des « Légionnaire du Christ » a fait savoir à la Commission que les coordonnées du jeune garçon figuraient bien dans son fichier et qu'elles avaient été radiées dès réception du courrier de la CNIL ; que le groupement concerné fait valoir que les coordonnées de Philippe avaient été obtenues par l'intermédiaire d'un aumônier qui les aurait lui-même recueillies directement auprès de l'intéressé lors d'un camp scout ; que le père de l'intéressé ne conteste pas cette version des faits ; que dans ces conditions, il n'y a pas lieu pour la Commission d'entreprendre auprès des Légionnaires du Christ la mission projetée ;

Considérant, s'agissant du journal « Français d'abord », que la mission de contrôle décidée par la Commission n'a pu à ce jour être entreprise ; qu'en effet, le Directeur administratif et financier du journal n'a pas répondu aux deux courriers qui lui ont été adressés par la CNIL, par lettre recommandée avec accusé de réception, lui demandant de préciser le lieu où se trouvait le fichier ; que l'adresse du journal ne fait état que d'une boîte postale, sans que son siège social puisse être localisé ; que le seul élément dont dispose la Commission pour déterminer le lieu exact où est tenu le fichier des destinataires de cette publication résulte d'un appel téléphonique, reçu par les services de la CNIL le 12 janvier 1999, d'une personne se présentant comme étant le directeur administratif et financier du journal « Français d'abord » précisant que « la CNIL serait surprise si elle savait où se trouvait ce fichier » ; que cet élément est insuffisant en l'état des moyens d'investigation dont dispose la CNIL pour lui permettre d'accomplir sa mission ;

Considérant que la SERP et le journal « Français d'abord » ont utilisé, à l'insu de l'intéressé et de son représentant légal, des informations, dont la présentation atteste qu'elles résultent de l'utilisation d'un traitement automatisé d'informations nominatives, sur l'origine desquelles ils ne se sont pas interrogés pour faire de la prospection ;

Considérant que la SERP ne conteste pas avoir pu utiliser des étiquettes-adresses qui lui auraient été communiquées par un tiers non identifié mais fait valoir qu'elle ne procède pas, dans ce cas, à l'enregistrement de ces données nominatives dans son fichier de clients ;

Considérant que la réponse du journal « Français d'abord » a consisté à réexpédier à la CNIL les courriers qui lui avaient été adressés lui demandant notamment de radier les coordonnées du jeune Philippe de son fichier, agrafés dans une même liasse portant la mention manuscrite, à l'encre rouge, « C'est fait » ; qu'il paraît résulter de cet envoi que les informations concernant le jeune Philippe avaient été enregistrées dans un traitement automatisé dont elles auraient été radiées à la suite de l'intervention de la CNIL ;

Considérant que l'utilisation d'informations nominatives par ces deux organismes qui ne pouvaient régulièrement en avoir connaissance est susceptible de constituer une collecte de données frauduleuse, déloyale ou illicite au sens de l'article 226-18 du code pénal ;

Considérant en outre que l'absence de réponse du journal « Français d'abord » aux deux courriers de la Commission lui demandant de lui faire connaître le lieu exact où se trouve le fichier des destinataires du journal ne permet pas à la Commission de conduire les investigations nécessaires pour s'assurer du respect des dispositions de la loi du 6 janvier 1978 ; qu'un tel refus, dans ces conditions, constitue une entrave à l'action de la Commission, au sens de l'article 43 de la loi du 6 janvier 1978 ;

En conséquence,

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

— de dénoncer au Parquet X pour n'avoir pas pris de précautions suffisantes pour empêcher que soient communiquées à des tiers qui n'ont pas à en connaître tout ou partie des informations nominatives issues d'un fichier automatisé ou non se rapportant à des chefs et cheftaines des scouts d'Europe de la « province de Provence », faits constitutifs de l'infraction visée par l'article 226-17 du code pénal ;

— de dénoncer au Parquet la société SERP et le journal « Français d'abord » pour avoir collecté et utilisé, à l'insu de la personne concernée et de son responsable légal, des informations nominatives dont ils ne pouvaient avoir régulièrement connaissance sous forme d'étiquettes-adresse issues d'un traitement automatisé d'informations nominatives, faits constitutifs de l'infraction visée par l'article 226-18 du code pénal ;

— de dénoncer au Parquet le journal « Français d'abord » pour, en n'ayant pas répondu à deux courriers adressés par lettre recommandée avec accusé de réception lui demandant de préciser le lieu où était mis en œuvre le fichier des destinataires de cette publication, avoir entravé l'action de la CNIL, faits constitutifs de l'infraction visée par l'article 43 de la loi du 6 janvier 1978.

La CNIL a procédé à une autre dénonciation en 1999 (cf infra chapitre 7).

C. 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 4 606 demandes d'accès indirect qui ont donné lieu à 7638 investigations.

	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	**1999**
Requêtes	69	182	562	531	374	282	243	320	385	401	**671**
Evolution (en %)	- 0,0	+ 1,64	+ 2,09	- 5	- 29	- 25	- 14	+ 31	+ 20	+ 4	**+ 67**

Jamais la CNIL n'a autant été saisie de demandes de droit d'accès aux fichiers de « police » ou de « renseignements ». La progression du nombre de requêtes instruites d'une année sur l'autre est de 67 %. Sans doute, le débat sur le fichier STIC (cf 19e rapport d'activité, p 63) et le fonctionnement en « vitesse de croisière » du système Schengen (SIS) expliquent-ils cette forte augmentation.

Les 671 demandes reçues par la CNIL en 1999 doivent conduire la Commission à accomplir plus de 1100 vérifications, une même requête concernant souvent plusieurs traitements ou fichiers.

Au cours de l'année 1999, 808 vérifications ont été effectuées [1], 90 % ont été opérées dans des fichiers relevant du ministère de l'Intérieur.

Les requérants saisissent le plus souvent 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'entravent 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	**725**
– renseignements généraux (RG)	270
– police judiciaire (PJ)	102
– police urbaine (PU)	102
– direction de la surveillance du territoire (DST)	40
– système d'information schengen (SIS)	210
Douanes (FNID)	**1**
Ministère de la Défense	**83**
– gendarmerie nationale (GEND)	36
– direction de la protection de la sécurité de la défense (DPSD)	19
– direction générale de la sécurité extérieure (DGSE)	15
– direction de la sûreté et de la protection du secret (DSPS)	13
Total	**808**

1 Ces 808 vérifications concernent des saisines reçues au cours des années 97, 98 et 99 ; la recherche d'une éventuelle fiche et son analyse requérant parfois plusieurs mois.

Le résultat des investigations qui ont été menées en 1999, à l'exclusion des fichiers des renseignements généraux (270), soit 538, est le suivant :

Service	PJ	PU	DST	SIS	FNID	GEND	DPSD	DGSE	DSPS	Total
pas de fiche	30	63	34	96	1	8	13	10	8	263
fiche sans suppression d'informations	60	36	6	68	-	27	4	5	4	210
suppression totale ou partielle d'informations	12	3	-	46	-	1	2	-	1	65
Total	102	102	40	210	1	36	19	15	13	**538**

A titre d'exemple, la Commission a été saisie d'une demande de droit d'accès aux fichiers de police à la suite d'un refus d'agrément de garde assermenté qui avait été opposé au demandeur par le préfet de Paris au motif « qu'il était connu des services de police pour violence volontaire en 1993 ». Il a résulté des investigations menées par la CNIL que le requérant a été fiché à tort par la police judiciaire en tant que « personne mise en cause » alors qu'il avait été victime de faits délictueux. C'est donc sur la base d'une information erronée que le préfet de Paris s'était fondé pour refuser l'agrément demandé. Après avoir obtenu la rectification de cette information, la commission a informé le préfet de Paris de la nécessité que la situation administrative de l'intéressé soit réexaminée, cela a été fait dans un sens favorable au plaignant qui a finalement pu obtenir son assermentation.

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 requérant.

En fait, 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, conformément aux termes auxquels la CNIL est tenue en application de l'article 39 de la loi, « qu'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 270 investigations menées en 1999 dans les fichiers des renseignements généraux :

	Investigations RG 1999	% du total des vérifications effectuées aux RG
Requérants non fichés aux RG	173	64 %
Requérants fichés aux RG	97	36 %
Total	270	100 %

Sur les 97 requérants fichés, les dossiers ont été communiqués dans les proportions suivantes :

	Requérants fichés aux RG	% sur le nbre de requérants fichés
Dossiers jugés non communicables	15	15,5 %
Communication refusée par le ministre de l'Intérieur	0	-
Communication acceptée par le ministre de l'Intérieur – communication totale – communication partielle	82 79 3	84,5 %
Total	97	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 les requérants sont domiciliés dans la région Ile-de-France ou, lorsque, domiciliés dans une autre région, ils font l'objet d'une fiche dans les services des renseignements généraux de la préfecture de police de Paris. Dans tous les autres cas, la communication est organisée au siège de la préfecture du département dans lequel est domicilié le requérant.

Parmi les 82 communications qui ont été effectuées en 1999, 35 ont eu lieu au siège de la CNIL et 47 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé. A la suite de ces communications, seulement 6 requérants ont rédigé une note d'observation qui a été insérée dans le dossier des renseignements généraux les concernant.

Evolution des investigations aux renseignements généraux

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

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 de l'article 109 et 114 de la convention Schengen, la CNIL a reçu, au cours de l'année 1999, 359 demandes d'accès aux fichiers du système d'information Schengen, soit quatre fois plus qu'en 1998.

Les requérants à l'origine de ces 359 saisines étaient de 32 nationalités différentes.

Algérie : 228	Maroc : 24	Sénégal : 4
Croatie : 4	Pakistan : 4	Turquie : 21
France : 5	Roumanie : 22	USA : 4

43 autres saisines proviennent des pays suivants : Biélorussie, Bosnie, Bulgarie, Congo, Croatie, Egypte, Guinée, Inde, Irak, Iran, Kosovo, Lituanie, Mali, Moldavie, Niger, Pologne, République Tchèque, Russie, Togo, Tunisie, Ukraine, Yougoslavie, Zaïre.

Parmi les 359 saisines :
— 88 personnes n'étaient pas signalées
— 61 personnes étaient signalées par la France
— 90 personnes étaient signalées par l'Allemagne
— 15 personnes étaient signalées par l'Italie
— 8 personnes étaient signalées par l'Espagne
— 4 personnes étaient signalées par la Grèce
— 1 personne était signalée par les Pays-Bas
— 68 dossiers n'ont pas fait, à la date de rédaction du présent rapport, l'objet d'investigations
— 24 saisines ont été clôturées en l'état, les requérants n'ayant pas transmis à la CNIL, après relance, les éléments nécessaires aux investigations (date et lieu de naissance).

Sur les 267 investigations conduites, 34 ont abouti à la suppression pure et simple du signalement dans Schengen, soit près de 13 % des cas ;
— 1 fiche supprimée avait été introduite par le bureau Sirène français
— 33 fiches supprimées avaient été introduites par le bureau Sirène allemand.

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

Bilan 1978 -1999

Au 31 décembre 1999, le nombre de traitements enregistrés par la CNIL depuis 1978 est de 700 833. Les traitements déclarés selon une procédure simplifiée représentent une part essentielle des formalités préalables (68,84 %), qui atteint plus de 69 % en 1999. Le nombre de déclarations de traitements à la CNIL a ainsi presque doublé depuis 1994. Il convient de relever aussi que le nombre de déclarations ordinaires n'a cessé d'augmenter, manifestant le succès de la politique de concertation et de sensibilisation de la CNIL envers les responsables de fichiers du secteur privé.

	1978 - 1999	% du total des formalités
Déclarations simplifiées et modèles types	503 170	68,845%
Demandes d'avis	37 785	5,170%
Déclarations ordinaires	159 141	21,774%
Demandes d'autorisation (chap Vbis - depuis 1997)	729	0,100%
Demandes d'autorisation (chap Vter - depuis 1999)	8	0,001%
Total des traitements enregistrés	**700 833**	-
Déclarations de modification	30 038	4,110%
Total des formalités préalables	**730 871**	100%

	1994	1995	1996	1997	1998	**1999**
Déclarations simplifiées et modèles types	27 827	46 549	60 355	53 953	50 735	**43 571**
Demandes d'avis	2 968	2 765	3 269	2 724	3 002	**3 538**
Déclarations ordinaires	5 926	7 812	9 727	10 326	11 333	**12 200**
Demandes d'autorisation (chap Vbis - depuis 1997)	-	-	-	133	244	**352**
Demandes d'autorisation (chap Vter - depuis 1999)	-	-	-	-	-	**8**
Déclarations de modification	1 928	1 777	3 428	2 639	2 358	**3 454**
Totaux	**38 649**	**58 903**	**76 779**	**69 775**	**67 672**	**63 123**

1999

Pour la période du 1er janvier au 31 décembre 1999, la CNIL a enregistré 63 123 nouveaux dossiers de formalités préalables, dont 3 454 concernent des déclarations de modification de traitements déjà enregistrés. La progression des déclarations ordinaires émanant du secteur privé (+7,65 %) et des demandes d'avis (+17,85 %) se poursuit.

	1999	% du total	rappel 1998	variation
Déclarations simplifiées et modèles types	**43 571**	69,025 %	50 735	- 14,12 %
Demandes d'avis	**3 538**	5,605 %	3 002	+17,85 %
Déclarations ordinaires	**12 200**	19,328 %	11 333	+7,65 %
Demandes d'autorisation (chap Vbis - depuis 1997)	**352**	0,558 %	244	+44,26 %
Demandes d'autorisation (chap Vter - depuis 1999)	**8**	0,012 %	-	-
Déclarations de modification	**3 454**	5,472 %	2 358	+46,48 %
Totaux	**63 123**	100 %	67 672	- 6,72 %

1) LES DEMANDES D'AVIS

L'article 15 de la loi du 6 janvier 1978 précise que les traitements du secteur public sont décidés par un acte réglementaire pris après avis motivé de la CNIL. Si l'avis de la Commission est défavorable, il ne peut être passé outre que par une décision de l'autorité compétente prise sur avis conforme du Conseil d'Etat (procédure jamais utilisée à ce jour). Si, au terme d'un délai de deux mois, délai qui peut être renouvelé une fois, l'avis de la Commission n'est pas notifié, il est réputé favorable (avis tacite).

La phase d'instruction des dossiers et la concertation qui s'engage entre la CNIL et le déclarant public aboutit, dans la grande majorité des cas, à des avis favorables ou réputés favorables.

La CNIL, qui a délivré plusieurs avis favorables assortis de réserves, a rendu, au cours de l'année 1999, un avis défavorable.

L'avis défavorable à l'utilisation des registres d'état civil à des fins de communication

Par délibération n° 99-024 du 8 avril 1999, la CNIL a rappelé aux maires qu'ils ne peuvent pas faire usage des informations portées sur les registres d'état civil à des fins de communication personnalisée, notamment à l'occasion de naissances, mariages et décès.

Saisie de cette question par le maire de Grenoble et, parallèlement, par l'un des conseillers de l'opposition municipale qui faisait valoir que si les registres d'état civil pouvaient être utilisés par le maire pour adresser, selon le cas, un mot de félicitations ou de condoléances à ses administrés, la même faculté devait être ouverte à l'ensemble des élus de la commune, la Commission a justifié l'avis défavorable

qu'elle a rendu par le principe de finalité des fichiers qui constitue une garantie essentielle au respect de la vie privée et de la tranquillité des personnes. De manière générale, ce principe s'oppose à ce que des informations enregistrées dans un fichier soient utilisées à des fins étrangères à celles qui ont justifié leur collecte et leur traitement. La Commission a en outre relevé que la tenue des registres d'état civil était confiée au maire ou à ses adjoints en leur qualité d'officier d'état civil et que les personnes concernées ne disposaient pas de la faculté de s'opposer à y figurer. La Commission a dès lors estimé que les données recueillies à l'occasion de l'exercice de cette mission de service public ne sauraient être utilisées à d'autres fins par qui que ce soit.

Cet avis défavorable confirme la doctrine constante de la CNIL en la matière, telle qu'elle a notamment été rappelée dans une recommandation du 3 décembre 1996 sur l'utilisation de fichiers à des fins politiques : « Chaque fichier public a une finalité particulière qui ne comporte pas celle de faire de la prospection politique ; les fichiers de gestion des collectivités territoriales qui sont susceptibles d'être utilisés pour la communication d'informations sur les activités et les réalisations de ces collectivités ne peuvent pas être utilisés à des fins de communication politique personnelle par les élus membres de cette collectivité » (cf 17e rapport d'activité, p. 140).

Dans le même sens, la CNIL avait également rendu un avis défavorable en 1997, à propos du projet d'un maire d'utiliser le rôle des impôts locaux de la commune pour adresser un courrier à ses administrés. La Commission avait notamment motivé son avis défavorable par le fait que ce courrier, qui mettait en cause les décisions d'une autre collectivité territoriale, était susceptible d'être interprété comme ayant une finalité politique (cf 18e rapport d'activité, p. 151). Toutefois, la Commission rappelle que, par dérogation à ces principes et depuis la loi n° 88-227 du 11 mars 1988 relative à la transparence financière de la vie politique, la liste électorale peut être librement communiquée à tout électeur, candidat ou groupement politique souhaitant s'adresser aux électeurs, sous réserve qu'il n'en soit pas fait un usage purement commercial.

Délibération n° 99-024 du 8 avril 1999 portant avis sur un projet d'arrêté du maire de Grenoble concernant l'envoi de courriers personnalisés aux administrés lors d'événements tels que les décès, naissances et mariages

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 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 articles 34 et suivants du code civil ;

Vu l'article 2122-32 du code général des collectivités territoriales ;

Vu l'instruction générale du 21 septembre 1955 relative à l'état civil, modifiée

Vu le projet d'arrêté municipal présenté par la mairie de Grenoble ;

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

Considérant que le maire de Grenoble a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis relative à la mise en œuvre d'un traitement automatisé dont l'objet est de permettre au maire et à son premier adjoint d'adresser à l'ensemble des administrés de la commune des courriers personnalisés à l'occasion d'une naissance, d'un décès ou d'un mariage ; que ces envois seraient réalisés à partir des informations portées sur les registres d'état civil par l'officier d'état civil à l'occasion des naissances, décès et mariages ;

Considérant que le code général des collectivités territoriales prévoit que le maire et les adjoints sont officiers d'état civil ; qu'à ce titre, le maire ou ses adjoints sont tenus de dresser acte, afin de leur conférer un caractère authentique, des naissances, mariages et décès ;

Considérant que le respect du principe de finalité des traitements s'oppose, de manière générale, à ce que des informations enregistrées dans un fichier soient utilisées à des fins étrangères à celles qui ont justifié leur collecte et leur traitement ; que la Commission estime, de doctrine constante, que ce principe de finalité constitue une garantie essentielle au respect de la vie privée et de la tranquillité des personnes tout particulièrement lorsque des fichiers publics sont en cause,

Considérant de surcroît que la tenue des registres d'état civil constitue une mission de service public confiée par la loi à l'officier d'état civil et que les personnes concernées ne disposent pas de faculté de s'opposer à y figurer ; que, dès lors, les données recueillies à l'occasion de cette mission ne sauraient être utilisées à d'autres fins par quiconque ;

Emet un avis défavorable au projet d'arrêté municipal présenté par le maire de Grenoble.

2) LES DEMANDES D'AUTORISATION

La loi n° 94-548 du 1er juillet 1994, qui a complété la loi du 6 janvier 1978 par un chapitre V bis, a institué un régime spécifique pour les fichiers de recherche en santé. En contrepartie d'une levée partielle du secret médical, cette loi a renforcé les procédures de contrôle sur ces fichiers. Leur création est en effet soumise à un régime d'autorisation par la CNIL, quel que soit le statut juridique de l'organisme responsable de la recherche — public ou privé —, après avis consultatif d'un comité chargé d'apprécier, sur le plan scientifique, la méthodologie de chaque projet de recherche faisant appel à un traitement informatique de données nominatives, la nécessité du recours à des données nominatives et la pertinence de celles-ci par rapport à l'objectif de la recherche.

La Commission a délivré ses premières autorisations en matière de recherche dans le domaine de la santé en 1997 et a, parallèlement, adopté un modèle de formulaire destiné à simplifier les procédures administratives qui

incombent aux organismes de recherche (cf 18e rapport d'activité, p. 202). En 1999, la CNIL a examiné 352 demandes d'autorisation en application du chapitre V bis de la loi du 6 janvier 1978.

Dans le souci de supprimer toute formalité excessive, la CNIL, en accord avec le comité, a admis que les demandes d'autorisation concernant les traitements mis en œuvre à l'occasion d'essais cliniques relevant de la loi « Huriet-Sérusclat » du 20 décembre 1988, puissent, sous certaines conditions, lui être présentées sous forme groupée. Cette procédure évite aux organismes d'avoir à constituer pour chaque recherche un dossier spécifique dans la mesure où les recherches biomédicales sont conduites dans le cadre d'exigences légales strictes et selon des méthodologies standardisées. Peuvent en bénéficier les traitements informatiques de données dites « indirectement nominatives » où l'identité n'est enregistrée que sous forme de numéro ou de code alphanumérique. En revanche, sont exclues de cette procédure allégée les recherches dont l'objet principal est l'étude des comportements, les recherches en génétique, et d'une manière générale, les recherches qui font apparaître l'identité complète des personnes.

Par ailleurs, la loi du 27 juillet 1999 portant création d'une couverture maladie universelle a complété la loi du 6 janvier 1978 par un chapitre V ter (art. 40-11 à 40-15), qui précise les conditions dans lesquelles des données de santé, qu'elles soient issues des professionnels de santé eux-mêmes, des systèmes d'informations hospitaliers ou des fichiers des caisses de sécurité sociale, peuvent être diffusées et exploitées à des fins d'évaluation des pratiques de soins et de prévention (cf loi 78-17 en annexe 5 et infra chapitre 5).

Tout en rappelant le principe d'anonymat qui doit présider à la transmission des données de santé tant aux autorités sanitaires qu'aux tiers, le nouveau chapitre V ter a confié à la CNIL le soin d'autoriser, sous certaines conditions, la communication de données indirectement nominatives, dès lors, notamment, qu'elles ne comportent pas les nom, prénom et numéro de sécurité sociale des patients.

Cette nouvelle procédure de demande d'autorisation préalablement à une diffusion de données de santé introduite par le chapitre V ter a été complétée par une modification du décret du 17 juillet 1978 (art. 25-24 à 25-30) qui a pour objet de préciser les règles de saisine de la CNIL, de fixer le contenu du dossier à présenter et de définir les modalités d'instruction et de délivrance des autorisations. En 1999, la CNIL a délivré 8 autorisations en application du chapitre V ter de la loi du 6 janvier 1978 (cf infra chapitre 5).

3) LES DÉCLARATIONS ORDINAIRES

Conformément à l'article 16 de la loi du 6 janvier 1978 qui fait obligation de déclarer à la CNIL les traitements créés dans le secteur privé, la Commission a reçu en 1999, 12 200 déclarations ordinaires.

Dès lors qu'un dossier de déclaration ordinaire est formellement complet au regard des dispositions de l'article 19 de la loi du 6 janvier 1978 et comporte

l'engagement par le responsable du traitement que celui-ci satisfait aux prescriptions de la loi, la CNIL est tenue de délivrer sans délai un récépissé de déclaration.

Cependant, conformément à la mission de conseil qu'elle tient de l'article 6 de la loi du 6 janvier 1978, la Commission s'attache, lorsqu'il lui apparaît que la mise en œuvre du traitement serait de nature à provoquer une violation de la loi ou à susciter des inquiétudes de la part des personnes fichées, à attirer l'attention du déclarant sur tel ou tel point.

4) LES DÉCLARATIONS DES SITES INTERNET

Dans un souci constant de sensibiliser les internautes et les responsables de sites aux questions de protection des données, la CNIL multiplie ses actions de pédagogie au regard de l'internet. Ainsi, après avoir dévoilé sur son site web comment chacun est pisté sur la toile — « Vos traces sur internet » — et diffusé un guide pratique — « Je monte un site internet » —, la Commission a proposé un formulaire de déclaration spécialement adapté aux traitements mis en œuvre dans le cadre d'un site internet (cf 18e rapport d'activité, p. 32 et 343 et 19e rapport d'activité, p. 20).

Ce formulaire, qui a vocation à simplifier les démarches préalables à la collecte et à l'utilisation de données personnelles en tenant compte des spécificités de l'internet, est disponible à partir du site de la CNIL à l'adresse http://www.cnil.fr.

L'accueil favorable réservé à cette procédure de déclaration, d'abord adoptée à titre expérimental, a conduit la CNIL à l'approuver définitivement par délibération n° 99-041 du 8 juillet 1999 (cf annexe 6).

En 1999 la CNIL a enregistré 2562 déclarations de sites internet. Ce sont ainsi 3 759 sites internet qui avaient été recensés à la CNIL au 31 décembre 1999, et il faut souligner que le rythme des déclarations de sites internet augmente rapidement pour atteindre une moyenne mensuelle de 300 déclarations.

	1997	1998	**1999**	**Total**
Déclarations sites internet	267	930	**2 562**	**3 759**

5) LES NORMES SIMPLIFIÉES ET MODÈLES TYPES

En 1999, la CNIL a reçu 43 571 déclarations de conformité à une norme simplifiée ou à un modèle type. Ce sont ainsi plus de 500 000 formalités préalables qui ont été accomplies selon des procédures allégées en 20 ans.

Normes simplifiées

En application de l'article 17 de la loi du 6 janvier 1978, la CNIL peut édicter, pour les catégories les plus courantes de traitements, des normes simplifiées qui permettent aux déclarants de s'acquitter des formalités préalables sous une forme

aussi légère que possible. Élaborées en vertu du pouvoir réglementaire de la Commission, ces normes visent à faciliter les procédures de déclaration. Lorsqu'un traitement relève d'une catégorie de traitements visés par une norme simplifiée, le responsable du fichier est simplement tenu, par le deuxième alinéa de l'article 17 de la loi, de déposer une déclaration de conformité à cette norme simplifiée. En cas de doute sur la conformité, la CNIL peut inviter le déclarant à justifier de celle-ci et, à défaut, lui demander de présenter une déclaration ordinaire ou une demande d'avis. En l'absence de doute sur la conformité, le dossier est immédiatement validé.

Depuis sa création, la CNIL a édicté 41 normes simplifiées et 488 949 traitements ont donné lieu à des déclarations en référence à l'une de ces normes. En 1999, plusieurs normes ont été modifiées dans le sens d'une plus grande simplification des formalités, principalement par la suppression de l'obligation d'annexer à la déclaration certains documents complémentaires. Les normes visées par les modifications sont les suivantes :
— la norme n° 9 concernant la gestion de prêts de livres (cf délibération n° 99-027 du 22 avril 1999, annexe 6) ;
— la norme n° 21 relative à la gestion des biens immobiliers (cf délibération n° 99-027 du 22 avril 1999, annexe 6) ;
— la norme n° 23 concernant la gestion des membres des associations à but non lucratif régies par la loi du 1er juillet 1901 (cf délibération n° 99-026 du 22 avril 1999, annexe 6) ;
— la norme n° 36 concernant la liquidation et le paiement des rémunérations des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public (cf délibération n° 99-025 du 22 avril 1999, annexe 6) ;
— la norme n° 37 concernant la gestion des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public (cf délibération n° 99-025 du 22 avril 1999, annexe 6).

Modèles types

La procédure de déclaration de conformité à un modèle type est régi par l'article 29 du règlement intérieur de la CNIL qui précise que lorsqu'un traitement est destiné à être mis en œuvre, dans des conditions identiques, par plusieurs services d'une administration ou d'un organisme public, un modèle type peut être présenté à la Commission. Dans ce cas, l'avis favorable rendu sur le modèle type permet à chaque utilisateur du traitement d'effectuer une simple déclaration de conformité au modèle standard.

Depuis 1978, 290 modèles types ont reçu un avis favorable de la Commission et 14 221 traitements ont donné lieu à de simples déclarations en référence à l'un de ces modèles. En 1999, la CNIL a adopté un nouveau modèle type dans le secteur de la justice relatif à l'informatisation du suivi des affaires pénales par le Parquet général des cours d'appel (cf délibération n° 99-029 du 4 mai 1999 en annexe 6).

L'arrêté du Garde des Sceaux, ministre de la Justice, du 18 juin 1999, fait cependant l'objet de plusieurs recours pour excès de pouvoir formés notamment par l'Ordre des avocats de Paris et la Fédération nationale de l'Union des jeunes avocats qui font reproche à cette informatisation des Parquets généraux de conduire à enregistrer pendant un délai de cinq ans les nom, prénoms et numéro de téléphone professionnel des avoués, avocats et huissiers intervenant dans les procédures dont la cour d'appel a à connaître.

II. DEUX DÉBATS DE SOCIÉTÉ

A. Le fichier national des empreintes génétiques

C'est la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs qui a créé le premier fichier national d'empreintes génétiques en matière criminelle. La CNIL, qui n'avait pas été consultée sur ce projet — et qui n'avait, formellement, pas à l'être, le principe du fichier résultant d'un amendement parlementaire, et non pas du projet de loi lui-même — a été saisie pour avis, en juillet 1999, des mesures d'application prises par décret en Conseil d'Etat.

Dès avant l'adoption par le Parlement de la loi du 17 juin 1998, la Commission avait procédé, dans le cadre général de sa mission de veille et de prospective, à une étude des droits et pratiques comparés en matière d'identification criminelle par empreintes génétiques et effectué plusieurs visites sur place dans des laboratoires de génétiques agréées, laboratoires privés ou hospitalo-universitaires, le laboratoire de police scientifique de Paris ainsi qu'à l'Institut de recherche criminelle de la gendarmerie nationale à Rosny-sous-Bois. Ces visites sur place ont permis à la Commission de recueillir l'opinion des professionnels concernés, de se faire une idée très précise des techniques d'analyses, de leur évolution possible, ainsi que des pratiques suivies, notamment pour la conservation des analyses et des scellés.

1) L'ADN ET LES ANALYSES D'IDENTIFICATION

L'ADN a été découvert en 1944 comme constituant un élément essentiel du matériel héréditaire. L'ADN du noyau de chacune de nos cellules (ADN nucléaire) détermine toutes nos caractéristiques organiques, morphologiques et parfois pathologiques : cet ADN nucléaire détermine notre identité. Il se présente sous la forme d'un très long filament, enroulé sur lui même, comme une double hélice, formée d'une succession de bases qui sont des sous-unités chimiques au nombre de quatre. C'est la fréquence d'alignement des paires de bases qui est propre à chaque individu et permet de différencier un individu d'un autre. C'est en 1953 que MM. Watson et Crick ont établi le schéma de la structure en double hélice de l'ADN.

L'ADN des chromosomes d'une cellule humaine formant le génome comporte environ 3 milliards de paires de base qui se font face deux à deux, et mesurerait, déroulé, 1,80 m. Une partie de cet ADN, représentant 10 à 20 % du tout, est le

support de l'information sous forme d'unités dites « codantes » dans la mesure où elles sont constituées de gènes qui sont responsables de toutes nos caractéristiques organiques, physiologiques et morphologiques. La plus grande partie de l'ADN nucléaire, dont, en l'état de la science, on ne connaît pas la fonction précise, est dite « non codante ».

C'est le professeur Alec Jeffreys qui a découvert en 1984 les possibilités nouvelles liées, notamment dans le domaine des recherches judiciaires, à cette séquence spécifique à chaque individu, et que l'on appelle communément « l'empreinte génétique ».

Ces découvertes ont été assez rapidement exploitées en France et à l'étranger pour permettre d'identifier des individus dans deux grands domaines, d'une part, la recherche en paternité, d'autre part, les recherches criminelles.

Le caractère spectaculaire des résultats judiciaires obtenus est incontestable. Chacun a ici le souvenir d'un père présumé dont l'analyse de l'empreinte génétique — prélevée sur son cadavre — a permis d'exclure, post mortem, qu'il puisse être celui d'une jeune fille qui, pourtant, paraissait lui ressembler. Le nombre de personnes innocentées grâce à des comparaisons d'empreintes génétiques vient récemment de conduire les Etats-Unis à entreprendre une réflexion sur les délais de prescription en matière de révision des procès, voire à suspendre l'exécution de personnes condamnées à mort. Parallèlement, certains juges d'instruction français n'ont pas hésité à inviter toute la population d'une commune ou d'un canton à se soumettre à des prélèvements afin de pouvoir identifier, par le recours massif à l'analyse génétique, l'auteur d'un viol.

Bien qu'il s'agisse encore de méthodes récentes, sur le plan scientifique, leurs résultats sont de plus en plus recherchés sans qu'aucune contestation sérieuse ne leur soit opposée.

Aujourd'hui, la présentation des résultats d'un profil génétique, qui a pu initialement être exprimée sous la forme de « codes barres », est exprimée sous la forme d'une série de chiffres qui représentent la taille des deux fragments d'ADN pour une région donnée.

2) LES ANALYSES D'ADN ET LE DROIT

Depuis une quinzaine d'années, les analyses ADN sont pratiquées dans le cadre de procédures judiciaires. Ce cadre juridique dans lequel peuvent avoir lieu, en France, les prélèvements et les analyses, n'est en rien modifié par la loi du 17 juin 1998 qui crée le fichier national.

Les conditions légales d'un prélèvement

Le prélèvement de matériel biologique sur la personne est soumis au principe de l'inviolabilité du corps humain. Ce principe a été consacré, dans l'article 16-1 du code civil, par la loi du 29 juillet 1994 relative au respect du corps humain. Il interdit de procéder à des prélèvements sans le consentement de la personne. Il résulte de

ces dispositions qu'un prélèvement qui suppose un acte « invasif » sur le corps humain, tel qu'une prise de sang, un prélèvement capillaire ou un prélèvement buccal ne peut être effectué de force sur une personne.

Les travaux préparatoires des lois bioéthiques de 1994 attestent cependant que la discussion parlementaire sur ce point fut difficile et complexe. Le gouvernement de l'époque avait d'ailleurs introduit un amendement selon lequel « en matière pénale, le consentement de l'intéressé n'est pas requis » (JO page 5870), amendement qui fut adopté en première lecture par l'Assemblée Nationale. C'est à l'occasion des discussions devant le Sénat et d'une refonte complète du texte proposé pour l'article 16-11 que cet amendement a été supprimé. En doctrine, certains auteurs estiment que le Parlement a ainsi considéré que l'absence de consentement correspondait aux principes généraux applicables en procédure pénale et qu'il n'y avait donc pas lieu, dans ce domaine, de subordonner le prélèvement au consentement des personnes concernées. La doctrine majoritaire, comme d'ailleurs la Chancellerie, estime au contraire que le principe de l'inviolabilité du corps humain est un principe général auquel le code de procédure pénale n'apporte nulle dérogation et qu'à défaut de disposition législative expresse autorisant, dans certains cas, un prélèvement forcé, tout prélèvement doit obéir au principe du consentement de la personne.

En tout état de cause, le respect de ce principe d'inviolabilité du corps humain n'interdit pas de ramasser sur le lieu d'un crime ou d'un délit du « matériel biologique » (un cheveu, un poil, une tâche de sang, du sperme, de la salive sur le bout filtre d'une cigarette) qui se serait naturellement détaché du corps humain. Dans ce cas là, nul besoin évidemment de recueillir le consentement préalable de la personne.

Les conditions légales de l'analyse de l'ADN

Ce qui est en cause à ce stade n'est plus le prélèvement d'un échantillon biologique, c'est l'analyse elle-même. En effet, les conditions légales de l'analyse ne sont pas les mêmes en matière civile ou en matière pénale.

En matière civile, aucune analyse d'ADN ne peut être faite sans le consentement de la personne. C'est donc la règle du « double consentement » qui prévaut : consentement au prélèvement et consentement à l'analyse. L'article 16-11 du code civil, dans ses deuxième et troisième alinéa, précise en effet que l'identification génétique d'un individu, c'est-à-dire l'analyse de son ADN, réalisée en exécution d'une mesure d'instruction ordonnée par le juge saisi d'une action en établissement ou contestation d'un lien de filiation, ou en matière d'obtention ou de suppression de subsides, doit être précédée du consentement préalable et exprès de la personne. De même, lorsque l'identification est effectuée à des fins médicales ou de recherche scientifique, le consentement de la personne doit être au préalable recueilli.

En matière pénale, la règle du double consentement ne s'applique pas. L'analyse aux fins d'identification par empreinte génétique — une fois le matériel biologique obtenu — ne nécessite pas l'accord de l'intéressé.

L'analyse génétique obéit alors aux règles spécifiques à la procédure pénale selon le cadre procédural dans lequel elle prend place (enquête préliminaire, enquête de flagrance, expertise ordonnée par le juge d'instruction ou par la juridiction de jugement).

Les conditions d'agrément des personnes habilitées à effectuer des identifications génétiques en matière pénale

Seules sont habilitées à procéder à des identifications par empreintes génétiques les personnes ayant fait l'objet d'un agrément dans des conditions fixées par un décret en Conseil d'Etat du 6 février 1997. Lorsque les identifications sont ordonnées dans le cadre d'une procédure judiciaire, ces personnes doivent, en outre, être inscrites sur une liste d'experts judiciaires.

L'agrément est délivré par une commission instituée auprès du Garde des Sceaux et présidée par un magistrat de la Cour de cassation qui comporte par ailleurs dix membres nommés en fonction de leur qualité ou de leur compétence.

Les conditions d'agrément sont nombreuses et rigoureuses. Ainsi, l'agrément est attribué pour une durée de cinq ans et fait l'objet d'un réexamen à l'issue de cette période. Un contrôle de qualité organisé sous l'autorité de l'Agence du médicament est effectué deux fois par an et est notamment « destiné à assurer la fiabilité des résultats des analyses biologiques d'identification par empreintes génétiques ».

Le décret de 1997 impose également aux laboratoires de répondre à certaines conditions. Ainsi, pour pouvoir être agréé, le laboratoire doit disposer d'infrastructures et d'équipements adaptés aux techniques de biologie moléculaire de façon à garantir l'absence de toute contamination. Les locaux affectés à la conservation des scellés, des échantillons biologiques et des résultats d'analyses doivent être équipés d'installations propres à garantir la sécurité et la confidentialité.

Les personnes physiques ou morales titulaires de cet agrément sont, à la date de rédaction du rapport, au nombre de 21.

3) UNE RELATIVE PRUDENCE

La genèse de la loi française manifeste une grande prudence à l'égard de la constitution des fichiers d'empreintes génétiques à des fins d'identification criminelle.

Ainsi, la première proposition de loi sur le sujet n'a été déposée sur le bureau de l'Assemblée Nationale qu'en décembre 1996. Le champ d'application de cette proposition de loi était au demeurant fort limité puisque, si elle visait à la fois les personnes condamnées et les suspects, c'est-à-dire des personnes mises en cause pendant l'enquête, elle ne concernait que les infractions sexuelles et seulement une partie d'entre elles, celles commises sur des mineurs de moins de quinze ans.

Prudence encore quand le Gouvernement de l'époque n'a pas inscrit cette proposition à l'ordre du jour de l'Assemblée Nationale.

La même prudence s'est manifestée lors du débat sur le projet de loi relatif à la prévention et à la répression des infractions sexuelles quand, dans un premier temps au moins, la commission des Lois de l'Assemblée Nationale a rejeté un premier amendement tendant à la création d'un fichier national des traces et empreintes génétiques des délinquants sexuels.

Enfin, cette prudence a constamment marqué les débats parlementaires et a conduit le législateur à exclure que les empreintes génétiques des personnes seulement suspectées voire mises en examen soient enregistrées dans le fichier national, ce dernier devant en définitive comporter les seules empreintes génétiques des personnes condamnées pour un crime ou un délit sexuel ainsi que les traces de matériels biologiques retrouvées sur le lieu du crime ou du délit, c'est-à-dire l'empreinte génétique des auteurs inconnus d'infraction.

Cette prudence n'est pas spécifiquement française

La recommandation du Conseil de l'Europe du 10 février 1992 sur l'utilisation des analyses d'ADN dans le cadre du système de justice pénale appelle l'attention des Etats-membres sur plusieurs principes tels que le principe de non-utilisation des analyses d'ADN aux fins de médecine prédictive, la nécessité de recueillir le consentement des personnes concernées, sauf décision judiciaire contraire, la nécessité de garantir la protection des données personnelles, le principe de destruction des échantillons analysés, sauf exceptions, la nécessité de mettre en place une procédure de contrôle et d'agrément des laboratoires habilités à procéder aux analyses.

De même, un texte adopté le 9 juin 1997 par le Conseil de l'Union européenne relatif à l'échange des analyses d'ADN en matière pénale préconise que les données analysées proviennent de segments non-codants de la molécule d'ADN et l'adoption de garanties spécifiques en faveur des personnes.

Au demeurant, contrairement à une idée reçue, les pays disposant d'un fichier national d'empreintes génétiques à des fins d'analyses criminelles, sont encore rares en Europe, la Grande-Bretagne et les Pays-Bas faisant, en la matière, figure de pionniers.

Cette prudence s'explique facilement

Le domaine de la recherche génétique et de l'exploitation de ces recherches à des fins d'identification de personnes soulève de nombreux problèmes éthiques comme les travaux préparatoires des lois bioéthiques de 1994 l'ont attesté, en consacrant d'ailleurs dans l'article 16-1 du code civil le principe d'inviolabilité du corps humain.

Actuellement, la recherche d'empreintes génétiques est effectuée sur la partie dite « non codante » de l'ADN, mais tout indique que les progrès de la science permettront à plus ou moins long terme de déterminer la fonction précise de la partie de l'ADN qui est dite aujourd'hui non codante. Il est d'ores et déjà possible de déterminer à partir de trois ou quatre marqueurs l'origine géo-ethnique d'un individu. Est-il admissible ou ne le serait-il pas de demander à un laboratoire de préciser, à partir

d'une trace découverte sur le lieu du crime (un cheveu, du sang, du sperme), l'origine ethnique supposée de l'auteur de l'infraction ?

S'agissant plus particulièrement de l'identification génétique à des fins de recherches criminelles, le risque de voir se constituer la photographie ou la carte du patrimoine génétique de criminels, de pouvoir déduire de cette photographie, par des calculs statistiques ou de probabilités, des prédispositions génétiques au crime, la tentation d'identifier de telles prédispositions avant que le crime ne soit commis, sont autant de questions de la nature de celles qui hantent, depuis au moins les travaux du criminologue Césare Lombroso, au milieu du XIX^{e} siècle, le champ intellectuel de la criminologie.

Le succès même de ces techniques de révélation de l'ADN pourrait inciter à ficher le patrimoine génétique non-codant de toute une population au motif — non dénué de soutiens, même dans des démocraties à la tradition aussi assurée que le Royaume-Uni — que seuls les coupables auraient à redouter un tel projet, tous les autres pouvant y trouver bénéfice, et tout particulièrement le bénéfice majeur de pouvoir être immédiatement innocenté d'un crime dont ils pourraient être accusés à tort.

Enfin, la constitution d'un fichier d'empreintes génétiques de criminels, auteurs inconnus de crimes, suspects ou condamnés, soulèvent les questions « classiques » des fichiers constitués à des fins d'identification criminelle. La photographie ou l'empreinte digitale d'un suspect peuvent-elles être conservées alors que le suspect aurait été innocenté ? Quels sont les effets de l'amnistie sur un fichier de cette nature, qui est d'abord un fichier de « comparaison », de références ? Ne s'agirait-il pas d'un casier judiciaire parallèle et, finalement beaucoup plus redoutable ?

Sur l'ensemble de ces points, il convient de constater que le législateur s'est montré prudent, quitte à ne pas répondre à quelques questions.

4) LE DISPOSITIF RETENU

Le fichier créé par la loi sera mis en œuvre par la Direction centrale de la police judiciaire et placé sous le contrôle d'un magistrat qui disposera d'un accès permanent au fichier, du droit de se déplacer sur le site où seront stockées les informations et du droit d'ordonner l'effacement des empreintes dont la conservation serait illicite. La CNIL s'est félicitée qu'un tel fichier soit placé sous la responsabilité d'un magistrat de l'ordre judiciaire. Il va de soi cependant que les pouvoirs particuliers qui sont reconnus à ce magistrat s'exerceront sans préjudice des pouvoirs généraux que la CNIL tient de la loi du 6 janvier 1978 sur l'ensemble des fichiers.

Conformément à la loi, les catégories d'informations enregistrées concerneront, les unes, les profils génétiques établis à partir de traces trouvées sur les lieux du crime ou du délit et dont on n'a pas pu identifier à qui elles se rapportaient (ces traces ne sont donc jamais associées au nom d'une personne), les autres, les empreintes génétiques des personnes définitivement condamnées pour infraction sexuelle. Dans ce dernier cas, les nom, prénoms, date et lieu de naissance, filiation et sexe du condamné seront associés à son empreinte génétique, laquelle sera conservée quarante ans, soit la durée de conservation des informations enregistrées dans le casier judiciaire. Compte-tenu de la finalité spécifique de ce fichier et de son utilisation à

des fins d'identification criminelle, la Commission a considéré qu'une telle durée de conservation n'était pas excessive.

Dans le souci d'alimenter aussi efficacement que possible le fichier national ainsi constitué, le projet de décret a prévu que pourraient y figurer toutes les analyses d'empreintes génétiques antérieurement effectuées dans le cadre d'affaires pénales relatives à des infractions sexuelles, qu'il s'agisse de traces non-identifiées retrouvées sur les lieux du crime ou d'empreintes génétiques de personnes déjà condamnées. Le même souci a conduit le Gouvernement à prévoir que le procureur de la République pourra ordonner des analyses d'empreintes génétiques sur des personnes condamnées pour infractions sexuelles antérieurement à la publication de la loi du 17 juin 1998 dès lors que ces personnes continuent à purger leur peine ou, dans le cas contraire, dans un délai maximum de six mois à compter de la date à laquelle la condamnation est devenue définitive.

En aucun cas, et comme l'a prescrit le législateur, l'empreinte génétique de simples témoins ou de personnes mises en examen ne pourra être enregistrée dans le fichier national.

S'agissant des mesures de sécurité particulièrement impérieuses qui doivent entourer un fichier de cette nature, seuls des fonctionnaires de la sous-direction de la police technique et scientifique du ministère de l'Intérieur et les personnels de l'Institut de recherche criminelle de la Gendarmerie nationale, spécialement habilités et affectés au service mettant en œuvre le traitement, pourront procéder aux opérations de rapprochement entre une empreinte génétique résultant de l'analyse effectuée dans le cadre d'une recherche criminelle pour l'une des infractions sexuelles visées par l'article 706-47 du code pénal et les empreintes enregistrées dans le fichier, une traçabilité des consultation par suivi informatique étant bien évidemment mise en place. Enfin, dans le souci d'éviter toute erreur dans la saisie de la série de chiffres qui constitue l'empreinte génétique, une double saisie sera effectuée par deux opérateurs distincts avant tout enregistrement au fichier national.

Enfin, le projet de décret a créé un service central chargé de centraliser les scellés, placé sous la responsabilité de l'Institut de recherche criminelle de la Gendarmerie nationale. Une telle centralisation existe dans de nombreux pays, même lorsqu'aucun fichier national n'est mis en œuvre. La CNIL a toutefois estimé que le texte qui lui était soumis devait être précisé afin qu'il en résulte clairement que les échantillons biologiques ainsi regroupés obéissent au régime juridique des scellés. Cela signifie concrètement qu'en aucun cas le service central ne pourra procéder à des analyses sur ce matériel biologique et qu'il devra se borner à en assurer la bonne conservation, les scellés ne pouvant, le cas échéant, être réouverts que sur autorisation judiciaire.

5) L'AVIS DE LA CNIL

Au-delà de l'important travail d'instruction et de précision des termes que la Commission a entrepris en liaison avec le ministère de la Justice sur le projet de décret dont elle était saisie, la CNIL s'est principalement attachée à exiger que le décret

précise que les analyses destinées à l'identification par empreintes génétiques ne portent que sur des segments d'ADN ne permettant pas de déterminer les caractéristiques organiques, physiologiques ou morphologiques des personnes concernées, à l'exception du marqueur qui identifie le sexe.

Cependant, au-delà de son avis sur le texte, la Commission a souhaité appeler l'attention du ministère de la Justice sur le sort à réserver aux autres analyses génétiques pratiquées dans le cadre d'une procédure pénale. La loi du 17 juin 1998 a en effet une portée limitée. Les garanties qu'elle apporte sont sérieuses. Mais que deviennent les autres analyses génétiques, celles pratiquées sur des personnes suspectées ou de simples témoins qui sont parfois appelés en masse, par certains juges d'instruction, à se soumettre à des analyses d'empreintes génétiques, celles enfin qui se rapportent à d'autres infractions que les seules infractions sexuelles visées par l'article 706-54 du code pénal ? Ces empreintes ne seront pas enregistrées dans le fichier national. Peuvent-elles ou doivent-elles être conservées dans les laboratoires, et, dans l'affirmative, sur quel fondement et sous quelles garanties ? Devront-elles être utilisées à des fins de rapprochement si elles ont été opérées dans le cadre de recherche en paternité, ou prélevées dans le cadre pénal sur de simples témoins. Toute empreinte obtenue est-elle bonne à conserver ? Il s'agit-là, après la première étape que constitue la mise en œuvre du fichier national, de questions vives encore à régler.

Délibération n° 99-052 du 28 octobre 1999 portant avis sur un projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques

La Commission Nationale de l'Informatique et des Libertés,

Vu le Convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pris ensemble le décret du 17 juillet 1978 ;

Vu la Directive 95/4 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 l'article 706-47 du code pénal ;

Vu le code de procédure pénale et notamment son article 706-54 ;

Vu les articles 16-1 et 16-11 du Code Civil ;

Vu le décret nº 97-109 du 6 février 1997 relatif aux conditions d'agrément des personnes habilitées à procéder à des identifications par empreintes génétiques dans le cadre d'une procédure judiciaire ;

Vu le projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques ;

Après avoir Monsieur Gérard Gouzes et Monsieur François Giquel, commissaires en leur rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Considérant que la Commission est saisie d'un projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques ;

Considérant que ce projet de décret est pris en application de l'article 28 de la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs qui a introduit un article 706-54 nouveau dans le code de procédure pénale créant un fichier national automatisé destiné à centraliser d'une part les empreintes génétiques des personnes condamnées et d'autre part les traces de matériel biologique retrouvées sur le lieu du crime ou du délit, les unes et les autres devant se rapporter aux seules infractions visées par l'article 706-47 du code de procédure pénale ; Considérant que l'article 706-47 du code pénal vise les infractions suivantes : le meurtre ou l'assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie, le viol, les agressions sexuelles autres que le viol, l'exhibition sexuelle, la corruption d'un mineur, la diffusion d'images pornographiques de mineurs, l'atteinte sexuelle sans violence, contrainte menace ou surprise sur un mineur de 15 ans et l'inceste sur un mineur de plus de quinze et non émancipé ;

Considérant que la loi autorise, à la demande du juge d'instruction ou du procureur de la République, le rapprochement des empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves et concordants de nature à motiver leur mise en examen pour l'une des infractions précitées avec les traces ou les empreintes génétiques enregistrées dans le fichier ; qu'elle fait toutefois interdiction de conserver dans le fichier national les empreintes génétiques de ces personnes ;

Sur les garanties devant entourer la réalisation des empreintes génétiques en matière pénale

Considérant que l'analyse de l'ADN ne constitue pas seulement un moyen biologique d'identification mais peut également révéler l'état de santé actuel ou futur d'une personne et en particulier sa prédisposition à telle ou telle pathologie ; que dans ces conditions, la constitution d'un fichier national automatisé des empreintes génétiques à des fins d'identification criminelle doit être entourée de toutes les garanties ;

Considérant que les analyses destinées à l'identification par empreintes génétiques ne doivent porter que sur des segments d'ADN ne permettant pas de déterminer les caractéristiques organiques, physiologiques ou morphologiques des personnes concernées ; qu'en l'état actuel de la science, la plus grande partie de l'ADN nucléaire est dite « non codante » dans la mesure où elle ne révèle aucune des caractéristiques précitées, seule la fréquence d'alignements de paires de bases constituant l'ADN — sous-unités chimiques au nombre de quatre — permettant de distinguer un individu de l'autre ;

Considérant que la Recommandation du Conseil de l'Europe du 10 février 1992 sur l'utilisation des analyses de l'ADN dans le cadre du système de justice pénale interdit l'utilisation aux fins de médecine prédictive des informa-

tions dégagées des analyses aux fins d'enquêtes et de poursuites pénales ; qu'une résolution du 9 juin 1997 adoptée par le Conseil de l'Union européenne relative à l'échange des résultats des analyses d'ADN précise que les empreintes génétiques doivent provenir « des segments non codants de la molécule d'ADN, dont on peut supposer qu'ils ne contiennent pas d'informations sur des caractères héréditaires spécifiques » ;

Considérant qu'il apparaît indispensable que le projet de décret précise explicitement que les empreintes génétiques qui figureront dans le fichier national doivent être réalisées, à l'exception du marqueur du sexe, à partir de segments non codants de la molécule d'ADN ;

Considérant que le Gouvernement propose en définitive que soit ajouté après l'article R 50-33 nouveau du projet de décret, un article ainsi rédigé :

« Les analyses destinées à l'identification par empreintes génétiques ne peuvent porter que sur des segments d'ADN non codants, à l'exception de celui correspondant au marqueur du sexe.

« Le nombre et la nature de ces segments d'ADN sont définis par arrêté du ministre de la Justice et du ministre de l'intérieur pris après avis de la commission chargée d'agréer les personnes habilitées à effectuer des missions d'identification par empreintes génétiques dans le cadre des procédures judiciaires, prévue par l'article premier du décret n° 97-109 du 6 février 1997 » ;

Considérant que cette rédaction satisfait la Commission ;

Sur le contrôle, par l'autorité judiciaire, du fichier national des empreintes génétiques

Considérant que le fichier national sera placé sous la responsabilité de la direction centrale de la police judiciaire du ministère de l'intérieur qui en assurera la gestion technique ; que le projet de décret précise que le magistrat sous le contrôle duquel sera placé le fichier sera le procureur général près la cour d'appel de Paris ;

Considérant que le procureur général se verra à ce titre reconnaître un accès permanent au fichier, la possibilité de se déplacer sur le site où seront stockées les informations et le pouvoir d'ordonner l'effacement des empreintes dont la conservation serait manifestement illicite ; que le projet de décret prévoit que ce magistrat pourra déléguer ses pouvoirs à un magistrat de la Cour d'Appel de Paris ; que ces dispositions doivent être regardées comme ne privant pas la CNIL, dans le cadre de ses missions générales de contrôle des fichiers, d'exercer les pouvoirs qu'elle tient de l'article 21 de la loi du 6 janvier 1978 ;

Considérant que le texte proposé pour l'article R 50-36 nécessiterait d'être complété afin de préciser que les pouvoirs propres du procureur général de Paris s'exercent « sans préjudice du contrôle exercé par la CNIL en application des dispositions et selon les modalités prévues par l'article 21 de la loi du 6 janvier 1978 » ;

Sur les catégories de données enregistrées

Considérant qu'il résulte des articles R 50-32 et R 50-33 nouveaux du projet de décret et du dossier de demande d'avis que les catégories d'informations enregistrées seraient, en ce qui concerne des profils génétiques établis à

partir de traces trouvées sur les lieux des crimes ou des délits, la nature de l'affaire et la référence de la procédure (enquête préliminaire, enquête pour crime ou délit flagrant ou instruction préparatoire dans le cadre des crimes ou délits mentionnés à l'article 706-47 du code de procédure pénale), le service ayant procédé au prélèvement et à la mise sous scellé, les lieu, date et numéro de scellés de prélèvement, les nom et prénoms de l'expert ayant procédé à l'analyse d'identification et la date de l'analyse, les régions de l'ADN analysées pour l'identification et les numéros de référence des fiches rapprochées ; que la fiche « trace » ainsi établie ne comportera pas l'identité de la personne, soit l'auteur inconnu de l'infraction, à laquelle se rapporte la trace ;

Considérant que, s'agissant des personnes définitivement condamnées, seront enregistrées les données suivantes : les noms, prénoms, date et lieu de naissance, filiation et sexe du condamné, les références de la transmission par laquelle le magistrat du ministère public a informé le responsable du fichier de l'autorisation d'enregistrement de l'empreinte génétique d'un condamné, les lieu, date et numéro du scellé du prélèvement, les nom et prénom de l'expert ayant procédé à l'analyse d'identification et la date de l'analyse et les régions de l'ADN analysées pour l'identification ;

Considérant que compte tenu des incidences que pourrait avoir une erreur dans la saisie des résultats d'analyses qui se présentent sous la forme de chiffres, aucune information ne sera enregistrée dans le fichier national sans que toutes les garanties nécessaires aient été préalablement mises en œuvre sous le contrôle des personnes habilitées pour assurer une fiabilité certaine des informations figurant dans le fichier ; qu'à cet égard, outre les mesures générales de sécurité et de contrôle qui entourent le fichier, il est prévu une double saisie des informations, les résultats ne pouvant être enregistrés que si les deux séries de chiffres saisies sont identiques ;

Sur la durée de conservation des données figurant au fichier central automatisé des empreintes génétiques

Considérant que la durée de conservation des informations enregistrées dans le fichier national est fixée à 40 ans ; ce délai court lorsqu'il s'agit de matériel biologique retrouvé sur le lieu de l'infraction, à compter de la date de l'analyse de la trace et, dans le cas des empreintes génétiques des condamnés, à compter du jour où la condamnation est devenue définitive dans la limite des 80 ans de la personne ;

Considérant, qu'eu égard à la durée des peines encourues par les personnes concernées cette durée ne paraît pas excessive au regard de la finalité particulière de ce fichier ;

Sur les catégories de personnes habilitées à interroger le fichier national

Considérant qu'aux termes de l'article R 50-37 nouveau du code de procédure pénale, les seules personnes dûment habilitées à consulter le fichier, l'alimenter et procéder aux opérations de rapprochement seront les fonctionnaires de la sous-direction de la police technique et scientifique du Ministère de l'Intérieur et les personnels de l'Institut de recherche criminelle de la Gendarmerie nationale spécialement affectés dans le service mettant en œuvre le traitement, implanté à Ecully dans le Rhône

Considérant que des mesures de sécurité physiques et logiques mises en œuvre pour contrôler l'accès au système informatique ; qu'ainsi une traçabilité des consultations par suivi informatique sera mise en place ;

Considérant qu'aucune interconnexion ou rapprochement avec un autre traitement automatisé d'informations nominatives n'est autorisée sous réserve des nécessités de fonctionnement du fichier détenu par l'Institut de recherche criminelle de la Gendarmerie nationale, organisme chargé, aux termes des dispositions de l'article R50-39 nouveau du code de procédure pénale, de la conservation des scellés comportant les prélèvements biologiques ;

Sur la création d'un service central de préservation des prélèvements biologiques

Considérant qu'aux termes de l'article R50-39 précité les échantillons de matériel biologique placés sous scellés pour l'une des infractions mentionnées à l'article 706-47 du code de procédure pénale, seront conservés par le service central de préservation de prélèvements biologiques de l'Institut de recherche criminelle de la Gendarmerie nationale à Rosny — sous-Bois ; qu'ainsi seront conservés non seulement les échantillons qui correspondent aux traces inconnues prélevées sur la scène de l'infraction ou aux empreintes génétiques des personnes condamnées, mais également les prélèvements biologiques effectués dans le cadre d'une procédure pénale ouverte du chef de l'une des infractions visées par l'article 706-47 du code de procédure pénale sur des témoins, des personnes suspectées ou des personnes n'ayant pas fait l'objet d'une condamnation définitive ;

Considérant qu'il y a lieu de préciser qu'une telle centralisation devra se limiter à la conservation des scellés et ne devra permettre en aucune façon au service central qui en a la charge de procéder pour son propre compte à une exploitation du matériel biologique ainsi centralisé ;

Considérant, dès lors, que le texte proposé pour l'alinéa premier de l'article R50-39 nouveau du code de procédure pénale devrait être ainsi rédigé : « Sur décision du procureur de la République ou, en cours d'information, du juge d'instruction, les scellés contenant des échantillons de matériel biologique saisis dans le cadre d'une enquête préliminaire, d'une enquête pour crime ou délit flagrant, ou d'une instruction préparatoire suivie pour l'une des infractions mentionnées à l'article R50-29, sont conservés, jusqu'à l'expiration des délais prévus par l'article R50-34, par le Service Central de Préservation des Prélèvements Biologiques de l'institut de recherche criminelle de la gendarmerie nationale à Rosny-sous-Bois » ; que le Gouvernement accepte cette rédaction ;

Sur les modalités d'alimentation du fichier central

Considérant que le projet de décret instituant le fichier national automatisé des empreintes génétiques prévoit les conditions d'alimentation initiales du fichier ;

Considérant que l'article 2 du projet de décret prévoit ainsi que les résultats d'analyses d'empreintes génétiques qui auront été réalisées antérieurement à l'entrée en vigueur de la loi et qui concernent des infractions énumérées par l'article 706-47 du code pénal ou aux infractions prévues par les articles 330 à 334-2 du code pénal dans leur rédaction antérieure au 1er mars 1994, pourront être enregistrées dans le fichier national des empreintes génétiques

dès lors qu'elles se rapportent à des traces inconnues ou à des personnes définitivement condamnées ;

Considérant en outre, que l'article R50-40 nouveau du code de procédure pénale prévoit que le procureur de la République pourra ordonner des analyses d'identification de personnes condamnées antérieurement à la mise en place du fichier pour l'une des infractions visées par la loi ;

Considérant que le procureur de la République pourra ordonner de telles analyses soit lorsque la personne condamnée est en cours d'exécution de peine soit, lorsque la personne a exécuté sa peine, dans les six mois suivant la date à laquelle la condamnation est devenue définitive ; que le ministère de la Justice propose de compléter ce texte en visant également, au titre des peines en cours d'exécution, le travail d'intérêt général et le régime de la libération conditionnelle ; que cette proposition n'appelle pas d'observation particulière de la part de la Commission ;

Considérant que, dans tous les cas où l'analyse sera ordonnée par le procureur de la République sur la personne d'un condamné, l'article R50-40 nouveau du code de procédure pénale impose de recueillir le consentement préalable de la personne concernée ;

Considérant que cette précision, qui résulte de l'application des dispositions de l'article 16-1 du code civil n'appelle pas d'observation de la part de la Commission ;

Considérant que le Gouvernement propose en définitive que les deuxième et troisième alinéas de l'article R 50-40 nouveau du code de procédure pénale soient ainsi rédigés :

« Cette analyse est ordonnée par le procureur de la République dans les six mois suivant la date à laquelle la condamnation est devenue définitive. Si en raison de sa condamnation, cette personne exécute une peine privative de liberté, un travail d'intérêt général, fait l'objet d'un sursis avec mise à l'épreuve ou se trouve placée sous le régime de la libération conditionnelle, cette analyse est ordonnée pendant la période d'exécution de peine ou le temps de l'épreuve.

« Le procureur de la République peut si nécessaire requérir un officier ou un agent de police judiciaire pour procéder ou faire procéder aux prélèvements destinés à l'analyse. Conformément aux principes posés par l'article 16-1 du code civil, ces prélèvements ne peuvent être effectués sur la personne du condamné sans son consentement » (le reste sans changement) ;

Considérant que cette proposition de rédaction n'appelle pas d'observation de la part de la Commission ;

Emet, sous la réserve ces observations, un avis favorable au projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques,

Constate que la mise en œuvre du fichier national automatisé ne tranche pas le sort à réserver aux résultats d'analyses génétiques qui sont pratiqués, dans le cadre d'une procédure diligentée pour l'une des infractions visées par l'article 706-47 du code de procédure pénale, sur de simples témoins ou sur des suspects, entendus comme des personnes à l'encontre desquelles existeraient des indices graves et concordants de nature à motiver leur mise en examen, ni aux résultats d'analyses génétiques qui sont pratiquées dans

le cadre de procédures pénales diligentées pour d'autres infractions que celles visées par l'article 706-47 du code de procédure pénale

Appelle, conformément aux dispositions de l'article 1er du décret du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978, l'attention des pouvoirs publics sur les conséquences de l'informatisation de l'activité des laboratoires agrées, et sur l'insuffisance des dispositions législatives et réglementaires encadrant l'activité des laboratoires et tout particulièrement les conditions de conservation et d'effacement des résultats d'analyse d'empreintes génétiques, qu'ils auraient, chacun pour ce qui le concerne, pratiquées sur réquisition judiciaire.

B. Les registres d'inscription des PACS

Le PACS (pacte civil de solidarité) aura fait couler beaucoup d'encre. La durée exceptionnelle des débats parlementaires — 9 octobre 1998, 13 octobre 1999 — le nombre d'amendements déposés, le large débat public qui a animé tous les secteurs de l'opinion, les manifestations de voies publiques qui ont mobilisé partisans et adversaires de la réforme législative qui allait devenir la loi du 15 novembre 1999, témoignent de la sensibilité du sujet.

La loi adoptée par le Parlement a introduit dans le livre 1er du Code civil relatif aux personnes un titre nouveau consacré au pacte civil de solidarité et au concubinage. Dans un cas comme dans l'autre, la loi précise clairement que le pacte civil de solidarité comme le concubinage peuvent concerner deux personnes physiques de sexe différent ou de même sexe.

La décision du Conseil Constitutionnel du 9 novembre 1999 et le nombre de réserves d'interprétation ou de précisions qu'elle comporte ne pouvait que renforcer l'idée qu'il s'agissait d'une réforme très novatrice, portant sur plusieurs sujets de société qui touchent tous à des questions fondamentales : l'intervention du droit dans les évolutions sociales, la place de la famille dans la société, les conséquences à attendre, à l'aube du troisième millénaire, des différents modes de vie en couple, le rapport entre le droit et la sexualité, enfin.

L'article 515-3 nouveau du Code civil prévoit l'inscription des déclarations de pacte sur un registre tenu au greffe des tribunaux d'instance, la loi précisant que le décret relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité est pris après avis de la CNIL. C'est en application de ces dispositions que la Commission nationale de l'informatique et des libertés a eu à se prononcer.

1) DESCRIPTION DU DISPOSITIF D'ENSEMBLE

Le PACS est un « contrat conclu par deux personnes physiques majeures, de sexe différent ou de même sexe, pour organiser leur vie commune » (article 515-1 nouveau du code civil).

L'article 515-2 nouveau du code civil interdit la conclusion d'un PACS, à peine de nullité, entre ascendants, descendants ou alliés en ligne directe ou

collatéraux jusqu'au troisième degré inclus. De même, il ne peut y avoir conclusion d'un PACS si l'un des partenaires est déjà engagé dans les liens du mariage ou est déjà lié par un PACS.

Il est à souligner que le Conseil Constitutionnel a considéré que la notion de « vie commune » ne recouvrait pas seulement une communauté d'intérêts et ne se limitait pas à l'exigence d'une simple cohabitation mais « suppose, outre une résidence commune, une vie de couple, qui seule justifie que le législateur ait prévu des causes de nullité du pacte qui, soit reprennent les empêchements à mariage visant à prévenir l'inceste, soit évitent une violation de l'obligation de fidélité découlant du mariage ».

Les partenaires du pacte sont, en outre, tenus par les termes de la loi (article 515-4 nouveau du code civil) de s'apporter une aide mutuelle et matérielle dont les modalités doivent être fixées par le pacte.

Le Conseil Constitutionnel a précisé à cet égard que l'aide mutuelle et matérielle devait s'analyser comme un devoir entre partenaires qui peuvent librement déterminer les modalités de cette aide, mais qui ne sauraient en exclure le principe. Le Conseil Constitutionnel a en effet précisé que « serait nulle toute clause de la convention méconnaissant le caractère obligatoire de cette aide ». Le Conseil Constitutionnel ajoute d'ailleurs que, dans le silence du pacte, il appartiendra au juge du contrat, en cas de litige, de définir les modalités de cette aide en fonction de la situation respective des partenaires.

Il a pu être justement dit que si le Conseil Constitutionnel avait « sexualisé » le pacte, il l'avait également « humanisé », comme en témoignent les précisions qu'il a apportées sur les conditions de la rupture du pacte : le pacte doit être un contrat loyal et le partenaire le plus vulnérable, protégé.

Les deux partenaires qui concluent un PACS doivent en faire la déclaration conjointe au greffe du tribunal d'instance dans le ressort duquel ils fixent leur résidence commune. Ils doivent fournir certains pièces justificatives, et notamment la convention passée entre eux, en double original, laquelle n'est pas conservée au greffe, les deux originaux étant visés par le greffier et aussitôt restitués aux partenaires.

S'agissant du PACS, le greffier du tribunal d'instance porte mention de la déclaration du pacte sur un registre spécialement tenu à cet effet. Il fait en outre porter cette mention sur le registre tenu au greffe du tribunal d'instance du lieu de naissance de chaque partenaire ou, pour les personnes nées à l'étranger, sur le registre tenu par le greffe du TGI de Paris.

Toute modification du pacte doit faire l'objet d'une déclaration conjointe inscrite au greffe du tribunal d'instance — ou auprès des agents diplomatiques et consulaires — qui a reçu l'acte initial auquel est joint l'acte portant modification de la convention.

Le PACS emporte plusieurs effets juridiques. Ainsi, les partenaires du PACS sont tenus solidairement des dettes contractées par l'un d'eux pour les besoins de la vie courante et pour les dépenses relatives au logement commun. A défaut de

précision contraire dans la convention liant les partenaires du PACS, les biens acquis à titre onéreux après la conclusion du pacte ou dont la date d'acquisition ne peut être établie sont réputés indivis par moitié.

Les partenaires liés par un pacte civil de solidarité font l'objet d'une imposition commune lors du troisième anniversaire d'enregistrement du pacte. Les partenaires bénéficient également d'abattements spécifiques pour les mutations à titre gratuit.

En matière de sécurité sociale, la personne liée par un PACS à un assuré social et qui se trouve à sa charge pourra demander le bénéfice de la qualité d'ayant droit de l'assuré pour l'ouverture du droit aux prestations en nature des assurances maladie et maternité.

Le bénéfice de plusieurs dispositions du code du travail est étendu aux partenaires d'un pacte, ainsi du droit pour deux partenaires liés par un pacte de prendre un congé simultané, de la possibilité de prendre un congé de deux jours pour le décès du partenaire. Dans le même esprit, les dispositions relatives au rapprochement de conjoints dans la fonction publique s'appliquent aux partenaires liés par un PACS.

Enfin, en cas d'abandon du domicile par le locataire, le contrat de location continue au profit du partenaire lié par un PACS. En cas de décès du locataire, le contrat de location est transféré au partenaire lié par un PACS. Parallèlement, le bailleur qui aurait conclu un pacte pourra donner congé à son locataire s'il envisage de reprendre le logement pour son partenaire.

S'agissant de sa dissolution, le pacte peut prendre fin soit par déclaration conjointe, soit sur décision unilatérale de l'un des partenaires, soit par le mariage de l'un des partenaires, soit évidemment par le décès (article 515-7 nouveau du code civil). Les partenaires procèdent eux-mêmes à la liquidation des droits et obligations résultant du pacte. A défaut d'accord, le juge statue sur les conséquences patrimoniales de la rupture.

2) L'AVIS DE LA CNIL

Un des problèmes les plus délicats que soulevait ce dossier était celui des règles de publicité ou de confidentialité qui devaient régir les registres tenus par les greffes. Chacun le sait, le grief a pu être fait à la loi, notamment par ceux qui contestaient la réforme, d'instituer des registres d'homosexuels. Les dérives auxquelles pourrait conduire la constitution de tels registres ont d'ailleurs été dénoncées par ceux-là mêmes parfois qui soutenaient l'idée que la logique de la loi devait conduire, nécessairement, à instituer des règles de publicité des registres calquées sur les règles de publicité des registres d'état civil.

Le Conseil Constitutionnel avait sur ce point précisé qu'il appartenait au pouvoir réglementaire compétent « d'apprécier les conditions dans lesquelles les droits des tiers concernés et le respect de la vie privée devaient être *conciliés* » et avait relevé, pour rejeter l'argument des requérants que la loi, en ayant institué de tels registres, aurait méconnu le principe du respect de la vie privée, et que devaient

s'appliquer à ces registres « les garanties résultant de la législation relative à l'informatique, aux fichiers et aux libertés ».

Aussi, le Gouvernement n'a-t-il pas fait le choix d'appliquer aux registres de pacs les règles de consultation des registres d'état civil. La CNIL n'a pu qu'approuver une telle orientation en soulignant d'une part, que l'on ne saurait tenir pour acquise, par le seul effet de la loi du 15 novembre 1999, la disparition des préjugés à l'égard des homosexuels, ni pour aboli tout risque de discrimination en raison des mœurs, d'autre part, que l'on ne saurait imposer aux personnes souhaitant conclure un pacs un régime de publicité qui aurait pour effet de rendre accessible à tous, et sans précautions particulières, des informations révélant leurs mœurs.

En revanche, il apparaissait légitime et nécessaire, en raison des effets juridiques attachés à la convention passée entre les partenaires, que la conclusion d'un pacte puisse être connue d'un certain nombre d'autorités, d'organismes, de services ou de personnes, tels l'autorité judiciaire, les notaires, les huissiers de justice, l'administration fiscale, les organismes débiteurs de prestations sociales.

Un problème s'est posé s'agissant des membres de la famille de chacun des partenaires. La finalité du registre justifiait-elle ou non que les ascendants, descendants, alliés en ligne directe et collatéraux jusqu'au troisième degré inclus (cousins germains) puissent avoir accès aux registres, comme le souhaitait la Chancellerie ? La Commission ne l'a pas souhaité et a été, en définitive, suivi sur ce point par le Gouvernement.

La Commission avait également émis des réserves sur le fait que les titulaires d'un droit de créance et les organismes de crédit puissent avoir accès, non pas à l'ensemble des informations figurant sur les registres, mais, comme le souhaitait la Chancellerie, au seul fait que le co-contractant ait ou non conclu un pacte. De la même façon, la CNIL avait fait une réserve sur le fait que les bailleurs puissent disposer d'un accès direct au registre. Il lui apparaissait en effet, sur ce dernier point, qu'un tel accès pourrait conduire certains bailleurs à être tentés de ne pas accorder un contrat de bail à une personne engagée dans les liens d'un pacte. Sur ces points, le Gouvernement a finalement limité le champ d'application de la disposition initialement envisagée. Ainsi, seuls pourront obtenir des greffiers d'instance l'information selon laquelle une personne est ou non « pacsée », « les titulaires d'un droit de créance né d'un contrat conclu pour la vie courante ou pour les dépenses relatives au logement ». Cela signifie en pratique qu'un bailleur de locaux ne saurait lors de la conclusion d'un bail avoir accès aux registres de pactes. En revanche, si le locataire ne règle plus ses loyers, le bailleur pourra consulter le registre pour savoir s'il est ou non engagé dans les liens du pacte.

La CNIL devait également examiner un projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi. Cet article subordonne l'enregistrement et la conservation de données sensibles dans un fichier au consentement exprès des personnes ou, pour des motifs d'intérêt public, à une autorisation faite par décret en Conseil d'Etat pris après avis conforme de la CNIL.

Le Gouvernement a sur ce point considéré que seul le rapprochement des prénoms pouvait révéler dans la plupart des cas le sexe des partenaires et donc leur

préférence sexuelle. Le souci du Gouvernement qu'un maximum de garanties entoure la tenue des registres de pactes a été partagé par la Commission.

Il convient sur ce point de s'arrêter sur un fait qui a pu être regretté par certains. La tenue des registres informatisés de pactes ne permet pas, en l'état, d'élaborer des statistiques en établissant une distinction entre couples hétérosexuels et couples homosexuels. Sans doute, la légitime curiosité sur les effets d'une réforme et l'intérêt des études sociologiques justifient-ils que des enquêtes puissent être menées sur cette nouvelle forme juridique de « vie de couple », pour reprendre l'expression retenue par le Conseil Constitutionnel. Sur ce point, toutefois le Gouvernement a estimé que la finalité des registres ne justifiait pas qu'un tri informatique en fonction de la nature du couple puisse être opéré, et qu'une fonction logicielle le permettant soit prévue dans le traitement d'informations. Ce parti pris est apparu, en l'état, pleinement justifié. Sans doute une telle précaution pourra-t-elle perdre de sa justification au fur et à mesure de l'évolution des mœurs.

Un dernier point a fait l'objet d'une réserve de la part de la Commission. Le projet du Gouvernement prévoyait en effet que des attestations de non-engagement dans les liens d'un pacte pourraient être délivrées à toute personne en faisant la demande. Cette disposition est apparue susceptible de conduire à de nombreuses dérives en permettant à certaines personnes ou organismes de l'exiger pour des motifs illégitimes et de créer, le cas échéant, des discriminations entre célibataires, partenaires d'un pacte, ou personnes mariées. La Commission relevait ainsi qu'il ne serait pas légitime, notamment, qu'un employeur exige la production d'une telle attestation lors d'une candidature à l'embauche, ni un bailleur lors de la conclusion d'un contrat de bail locatif. Le décret du 21 décembre 1999 limite, en définitive, la délivrance de tels certificats de « non-pacs » aux seules personnes souhaitant conclure un pacte et qui doivent, aux termes même de la loi, attester qu'elles ne sont pas déjà « pacsées ».

Délibération n° 99-056 du 25 novembre 1999 portant avis sur les projets de décret en Conseil d'Etat relatifs aux mesures d'application de la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité et à l'informatisation des registres d'inscription des pactes civils de solidarité

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 nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, le décret nº 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 la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité, ensemble la décision du Conseil Constitutionnel n° 99-419 du 9 novembre 1999 ;

Vu le projet de décret relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité et autorisant la création à cet effet d'un traitement automatisé des registres mis en œuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris et par les agents diplomatiques et consulaires français ;

Vu le projet de décret pris en application de l'article 31, alinéa 3 de la loi du 6 janvier 1978 ;

Vu le projet de décret pris en application de la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité et relatif à la déclaration, à la modification et à la dissolution du pacte civil de solidarité ;

Après avoir entendu M. Hubert Bouchet, Vice-Président délégué, en son rapport et Madame Charlotte-Marie Pitrat, Commissaire du Gouvernement, en ses observations ;

Considérant que la loi du 15 novembre 1999 relative au pacte civil de solidarité a introduit dans le Livre premier du code civil, relatif aux personnes, un titre XII intitulé « Du pacte civil de solidarité et du concubinage » ; qu'aux termes de l'article 515-1 nouveau du code civil le pacte civil de solidarité « est un contrat conclu par deux personnes physiques majeures, de sexe différent ou de même sexe, pour organiser leur vie commune » ; qu'en application de l'article 515-3, les personnes qui concluent un tel pacte en font la déclaration conjointe au greffe du tribunal d'instance dans le ressort duquel elles fixent leur résidence commune, cette déclaration étant inscrite sur un registre tenu par le greffe de ce tribunal ; que mention de cette déclaration doit également être portée sur un registre tenu au greffe du tribunal d'instance du lieu de naissance de chaque partenaire ou, pour les personnes nées à l'étranger, sur le registre tenu par le tribunal de grande instance de Paris ; qu'à l'étranger, l'inscription de la déclaration conjointe d'un pacte liant deux partenaires dont l'un au moins est Français est réalisée par les agents diplomatiques et consulaires français qui tiennent registre de ces déclarations ;

Considérant que l'article 15 de la loi susvisée renvoie les mesures d'application de ces dispositions à des décrets en Conseil d'Etat et précise que le décret relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à l'information, la modification du pacte civil de solidarité est pris après avis de la Commission Nationale de l'Informatique et des Libertés ;

Considérant qu'en application de ces dispositions, la CNIL est saisie d'un projet de décret autorisant la création d'un traitement automatisé des registres mis en œuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris et par les agents diplomatiques et consulaires français ainsi que d'un projet de décret portant application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 aux registres ainsi mis en œuvre ;

Considérant que le Gouvernement a également transmis à la CNIL, pour information, un projet de décret en Conseil d'Etat pris en application de la loi qui détermine notamment les conditions dans lesquelles peut être délivrée à

toute personne qui en fait la demande une attestation d'engagement dans les liens d'un pacte civil de solidarité ou une attestation selon laquelle cette personne n'est pas engagée dans les liens d'un pacte civil de solidarité ; qu'il y a lieu pour la Commission de porter appréciation sur les dispositions de ce texte qui sont en relation nécessaire avec les deux autres projets de décret ;

Considérant que le Conseil Constitutionnel a, dans sa décision 99-419 du 9 novembre 1999, d'une part, précisé qu'il appartiendra « au pouvoir réglementaire, compétent pour fixer les modalités d'application des dispositions [relatives à la publicité de la conclusion, de la modification et de la fin du pacte], d'aménager dans le décret prévu dans l'article 15 de la loi [...] l'accès des tiers aux différents registres de manière à concilier la protection des droits des tiers et le respect de la vie privée des personnes liées par un pacte » et, d'autre part, rejeté le grief de non conformité de la loi à la Constitution tiré de l'atteinte au respect de la vie privée au motif que « les conditions dans lesquelles seront traitées, conservées et rendues accessibles aux tiers les informations relatives au pacte civil de solidarité seront fixées par un décret en Conseil d'Etat pris après avis de la Commission Nationale de l'Informatique et des Libertés ; que s'appliqueront les garanties résultant de la législation relative à l'informatique et aux libertés » ; qu'il y a lieu de souligner que c'est « sous ces réserves » que le Conseil Constitutionnel a conclu que le législateur n'avait pas porté atteinte au principe du respect de la vie privée ;

Considérant que la Commission mesure pleinement le caractère novateur de la loi qui institue un nouveau contrat de vie de couple pouvant être conclu dans les mêmes conditions entre des personnes de même sexe ou de sexes différents ; que cette réforme qui attache des conséquences juridiques identiques aux contrats formés par des couples hétérosexuels et à ceux formés par des couples homosexuels témoigne d'une évolution des mœurs qui peut augurer la fin de certains préjugés défavorables à l'égard de personnes vivant en couple et ne souhaitant pas ou ne pouvant pas se marier ; que cependant on ne saurait aujourd'hui tenir pour acquise, par le seul effet du droit, la disparition de tels préjugés, ni pour aboli tout risque de discrimination en raison des mœurs ; que, dans ce contexte, et devant faire application aux registres d'inscription des pactes civil de solidarité des garanties qui résultent de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission doit veiller, comme l'a précisé le Conseil Constitutionnel, à ce que soient conciliés les droits des tiers concernés par la conclusion d'un pacte entre deux personnes et le respect de la vie privée des partenaires du pacte ;

Sur le projet de décret autorisant la création d'un traitement automatisé des registres

Considérant que le projet de décret énumère dans son article 3 les informations nominatives qui seront portées sur les registres ; qu'il s'agira des nom et prénoms de chacun des partenaires, de leur date et lieu de naissance, de l'adresse de leur résidence commune, de la date et du lieu d'inscription, qui confèrent date certaine au pacte, du numéro d'enregistrement de l'inscription, de la date d'enregistrement d'une éventuelle modification du pacte, de la nature et de la date de l'acte ou du fait générateur de la dissolution (déclaration conjointe de dissolution, signification par un partenaire d'une déci-

sion unilatérale de rupture ; mariage d'un des partenaires ou décès), de la date de notification ou de signification de la rupture et de la date de dissolution du pacte ; que le sexe des partenaires n'est pas enregistré sur les registres même si, dans la grande majorité des cas, il peut se déduire du prénom des partenaires ou d'autres mentions portées sur les registres telles que « né (e) » ; que pas davantage n'est conservée au greffe la convention passée entre les partenaires dont les deux exemplaires originaux sont, en application de l'article 515-3 nouveau du code civil, visés et datés par le greffier et restitués à chaque partenaire

Considérant que l'article 9 du projet de décret prévoit que les informations sont conservées sur les registres des greffes des tribunaux d'instance du lieu de naissance de chaque partenaire ou, s'il s'agit d'une personne née à l'étranger, sur le registre du greffe du tribunal de grande instance de Paris, pendant une durée de 30 ans à compter de la date à laquelle prend fin le pacte civil de solidarité ; que les mêmes informations seront effacées des autres registres sur lesquels elles figurent à l'expiration d'un délai de 5 ans à compter de la date de dissolution du pacte ; que la durée de conservation de 30 ans est justifiée par la prescription trentenaire en matière d'actions réelles et personnelles prévue par l'article 2262 du code civil ; qu'une telle durée est de nature à satisfaire à l'exigence, rappelée par le Conseil Constitutionnel, du respect des droits des tiers ainsi que, le cas échéant, des droits des deux partenaires concernés ;

Considérant que le projet de décret prévoit que les registres informatisés ne seront interconnectés avec aucun autre fichier et que seuls seront habilités à accéder aux informations nominatives portées sur les registres les fonctionnaires des greffes des tribunaux d'instance et du tribunal de grande instance de Paris ainsi que les agents diplomatiques et consulaires français que leurs missions et leurs compétences territoriales respectives habilitent à enregistrer, conserver, modifier ou communiquer à d'autres destinataires habilités ; qu'il y a lieu de prévoir, afin de renforcer la sécurité du traitement et d'empêcher toute tentative de consultation des fichiers à d'autres fins que celles pour lesquelles ils ont été constitués, qu'un système de journalisation informatique soit mis en place afin de conserver trace de toute consultation des registres informatisés ou de toute saisie ou modification des informations portées sur les registres ; que le ministère de la justice est disposé à mettre en œuvre un tel système ;

Sur le régime de publicité des registres

Considérant qu'il convient sur ce point de concilier, comme l'a précisé le Conseil Constitutionnel, la protection des droits des tiers et le respect de la vie privée des partenaires liés par un pacte ; que le Conseil Constitutionnel a précisé que la liberté, « droit naturel et imprescriptible de l'homme » « implique le respect de la vie privée » ; que l'accessibilité des registres du pacte dans des conditions identiques à celles qui régissent la publicité des registres d'état-civil ne serait pas justifiée et qu'il convient de l'aménager afin d'assurer le respect de la vie privée des personnes concernées ;

Considérant en effet, et en premier lieu, que le Conseil Constitutionnel a clairement indiqué que, compte-tenu de « l'objet voulu et défini par le législateur, la loi [instituant le pacte] est sans incidence sur les autres titres du Livre I du code civil, notamment ceux relatifs aux actes d'état-civil » ; qu'il y a lieu à

cet égard d'observer que le législateur, en confiant la tenue des registres de pactes à une autorité distincte de celle qui a en charge la tenue des registres d'état-civil, a souhaité manifester que la conclusion d'un pacte entre deux personnes n'avait aucune incidence sur leur état-civil ; que dès lors, aucune analogie ne saurait être faite entre les règles qui régissent la publicité de l'état-civil des personnes qui, comme l'a énoncé la Cour de Cassation, « est une base essentielle de l'ordre social » et celles qui doivent régir les registres de pactes ; que le Conseil Constitutionnel a d'ailleurs précisé que « la conclusion d'un pacte civil de solidarité ne donne lieu à l'établissement d'aucun acte d'état-civil, l'état-civil des personnes qui le concluent ne subissant aucune modification » ;

Considérant, en deuxième lieu, que la décision du Conseil Constitutionnel, en précisant que la notion de « vie commune », condition exigée par la loi pour autoriser la conclusion d'un pacte entre deux personnes, ne supposait pas seulement une résidence commune mais « une vie de couple », conduit à considérer que la conclusion d'un pacte, dans la mesure où elle peut concerner deux personnes du même sexe, révélera les orientations sexuelles des personnes ; que si les registres d'inscription de pactes n'ont pas « pour objet » comme l'a rappelé le Conseil Constitutionnel de « révéler les préférences sexuelles des personnes liées par un pacte », leur consultation pourrait permettre d'opérer une distinction entre les couples ; que l'outil informatique et les logiciels de recherche peuvent techniquement faciliter un tel tri sur la base des prénoms des partenaires concernés ou d'autres indications portées sur les registres telles que la formule « né (e) le… » ; que les nombreuses dispositions législatives ayant pour objet de proscrire toute discrimination fondée sur les mœurs des personnes attestent cependant la permanence d'un risque de discriminations et l'importance du trouble à l'ordre social que de telles discriminations peuvent provoquer ; que tel est le cas, en particulier, des dispositions relatives à l'embauche (article L. 123-1 et L.122-45 du code de travail) et, de manière plus générale, en matière de fournitures de biens et services (articles 225-1 et 2 du code pénal) ; que la directive européenne du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données inclut, dans son article 8, la « vie sexuelle » dans les « catégories particulières de données » dont le traitement est par principe interdit et qui, par dérogation à ce principe, appelle des garanties particulières ;

Considérant qu'au regard de ces textes, il ne saurait être imposé aux personnes qui souhaitent conclure un pacte civil de solidarité un régime de publicité qui aurait pour effet de rendre accessible à tous, et sans précaution particulière, des informations révélant leurs mœurs, privant ainsi les personnes concernées de la liberté de révéler ou non à leur entourage familial, personnel ou professionnel, leur choix de vie ; que le principe constitutionnellement protégé de liberté individuelle et le respect de la vie privée commandent que les personnes qui souhaitent s'engager dans les liens d'un contrat de droit privé déterminent elles-mêmes l'opportunité et le moment où elles souhaitent révéler l'existence d'un tel contrat et l'identité de leur partenaire dès lors que l'exercice de cette liberté ne cause aucun préjudice à autrui ;

Considérant en revanche qu'il est légitime, en raison des effets juridiques que la loi attache à la convention passée entre les partenaires, que la conclusion d'un pacte puisse être connue d'un certain nombre d'autorités, d'organismes, de services ou de personnes ;

Considérant qu'il en est ainsi, en premier lieu, de l'autorité judiciaire pour ce qui est des informations nécessaires au droit d'action du ministère public ou à l'instruction ou au jugement des litiges mettant en jeu l'existence, l'exécution ou la dissolution d'un PACS, compte-tenu notamment du rôle dévolu au Parquet civil en matière de constatation des empêchements de conclure un pacte, qui sont sanctionnés par la nullité absolue ; en deuxième lieu, des notaires pour les besoins des règlements successoraux et de l'établissement des actes nécessitant une publicité au bureau des hypothèques ainsi que des donations ; en troisième lieu, des agents chargés de l'exécution d'un titre exécutoire pour l'exercice de leur mission ; en quatrième lieu, des administrateurs judiciaires et des mandataires liquidateurs désignés dans le cadre d'une procédure de redressement ou de liquidation judiciaire ; en cinquième lieu, de l'administration fiscale agissant en vertu de son droit de communication prévu par l'article L 83 du Livre des Procédures fiscales, dans la mesure, notamment, où la loi attache à la conclusion d'un pacte plusieurs avantages fiscaux ; en sixième lieu, des organismes débiteurs de prestations familiales, de prestations d'assurance maladie, maternité et décès et des organismes débiteurs de l'allocation veuvage pour les informations strictement nécessaires à l'exercice du droit de contrôle des prestations versées ; en septième lieu, des tuteurs à l'égard des informations relatives à la personne dont ils assurent la tutelle, dans la mesure où l'article 506-1 nouveau du code civil prévoit qu'un majeur placé sous tutelle ne peut conclure un pacte

Considérant, en revanche, que le I-10° de l'article 5 du projet de décret prévoit que « les personnes concernées par l'article 515-2 nouveau du code civil susceptibles de demander l'annulation du pacte civil de solidarité » pourront obtenir communication des informations portées sur les registres de pactes ; que l'article du code civil auquel il est fait référence sanctionne de nullité tout pacte conclu (1°) entre ascendant et descendant en ligne directe, entre alliés en ligne directe et entre collatéraux jusqu'au troisième degré inclus, (2°) entre deux personnes dont l'une, au moins, est engagée dans les liens du mariage, (3°) entre deux personnes dont l'une, au moins, est déjà liée par un pacte civil de solidarité ; que l'article 515-2 du code civil vise, comme le précise la décision du Conseil Constitutionnel, à « assurer le respect des règles d'ordre public régissant le droit des personnes » ; que la référence faite à cet article par le projet de décret conduit à penser que l'objectif poursuivi est de permettre à certains proches des partenaires de pouvoir faire constater la nullité des pactes qui seraient conclus en méconnaissance de ces règles d'ordre public ; que la Commission observe que, s'agissant des causes de nullité visées par le 2° et le 3° de l'article 515-2 nouveau du code civil, le greffier recevant la déclaration conjointe sera en mesure, à partir des pièces obligatoirement produites par les futurs partenaires en application de l'article 515-3 nouveau du code civil, de s'assurer que le pacte ne concerne pas deux personnes dont l'une au moins serait mariée ou déjà liée par un pacte ; que, s'agissant des autres causes de nullité, visées au 1° de l'article 515-2 du code civil, le Procureur de la République pourra, à tout moment, dans un domaine qui touche à l'ordre public, d'initiative ou sur demande de toute personne qui viendrait à nourrir un doute sur la validité du pacte conclu, consulter le registre et faire constater l'éventuelle nullité du pacte ; qu'ainsi, l'objectif visé par la disposition du texte proposé paraît pouvoir être atteint sans qu'il soit nécessaire de prévoir une disposition d'ordre général du type de celle qui est envisagée par le projet de dé-

cret ; que, dans ces conditions, et pour ces motifs, la Commission ne saurait, en l'état du texte qui est proposé à son examen, accepter cette disposition ;

Considérant que le projet de décret prévoit que les organismes ci-dessus énumérés auront communication des informations issues des registres sous la forme d'une attestation qui comportera l'identité des partenaires, la date et le lieu d'inscription du pacte, la date des modifications éventuelles du pacte ainsi que la nature et la date de l'acte ou du fait générateur de la dissolution ; qu'il y a lieu à cet égard de relever que le Conseil Constitutionnel a précisé que les règles d'enregistrement des pactes avaient notamment pour finalité de « conférer date certaine au pacte civil de solidarité pour le rendre opposable aux tiers » ; que si la date de dissolution d'un pacte fait partie des informations nécessaires à la sauvegarde des droits des tiers concernés, l'information relative à la nature de l'acte ou du fait générateur de la dissolution qui est, dans son principe, sans incidence sur les droits des tiers concernés par le pacte, ne devra se présenter que sous la forme suivante : « décès » ou « autre cause de dissolution », à l'exclusion de toute autre mention de nature à divulguer que le pacte aurait été dissous par le mariage de l'un des partenaires, par une déclaration conjointe, ou de manière unilatérale ; qu'il y a lieu pour la Commission de faire une réserve sur ce point ***;***

Considérant que le projet de décret prévoit par ailleurs au II de son article 5 qu'un certain nombre de tiers pourraient avoir connaissance de la seule information selon laquelle une personne déterminée est engagée dans les liens d'un pacte ; que dans un tel cas, l'identité du partenaire ne serait pas communiquée à ce tiers ;

Considérant qu'il y a lieu d'observer que le caractère novateur de la réforme ayant institué le pacte ne saurait conduire, sans risque important de dérives et d'atteinte à la dignité des personnes, à ce que tous les actes de la vie courante justifient la consultation, fût-elle partielle, d'un registre de la nature de celui sur lequel sont inscrits les pactes ;

Considérant que la liste des tiers concernés qui pourraient bénéficier d'un tel accès aux registres appelle des réserves ;

Considérant, s'agissant des « titulaires d'un droit de créance né d'un contrat conclu pour les besoins de la vie courante ou pour les dépenses relatives au logement, aux fins de la sauvegarde ou du recouvrement de leur créance », visés au 1° du II de l'article 5 du projet de décret, que cette disposition se réfère nécessairement à celle de l'article 515-4 nouveau du code civil selon laquelle « les partenaires sont tenus solidairement à l'égard des tiers des dettes contractées par l'un d'eux pour les besoins de la vie courante et pour les dépenses relatives au logement commun » ; que si cette dernière disposition justifie pleinement que le titulaire d'une créance de cette nature puisse engager une action en recouvrement à l'égard du partenaire du débiteur, il demeure que les conditions concrètes de l'accès du créancier prévu par le projet de décret supposeraient que celui-ci rapporte, en sa qualité de demandeur, la preuve que la créance qu'il détient sur les partenaires a bien été contractée pour les besoins de la vie courante ou pour les dépenses relatives au logement commun, d'une part, est liquide et exigible, d'autre part, et que le greffier du tribunal d'instance qui tient le registre soit en mesure d'en juger ; que la mise en œuvre pratique d'une telle disposition est susceptible de soulever des difficultés dont le règlement ne peut être laissé à la seule appréciation du greffier tenant le registre ; que, dans ces conditions, et pour ces

motifs, la Commission ne peut, en définitive, en l'état du texte qui lui est soumis, accepter cette disposition ;

Considérant, s'agissant des organismes de crédit « pour ce qui concerne les personnes qui sollicitent ou à qui ils ont délivré un emprunt », que les mêmes observations et réserves doivent être faites même s'il ne paraît pas illégitime pour l'organisme de crédit de demander directement aux personnes qui sollicitent un crédit si elles sont ou non dans les liens d'un pacte ; qu'en tout état de cause, la finalité des registres ne saurait justifier qu'un organisme de crédit dispose d'un accès direct au registre, fût-il partiel ; qu'il y a lieu pour la Commission de faire une réserve sur ce point ;

Considérant, s'agissant des bailleurs de locaux, qu'un tel accès pourrait être de nature à permettre aux bailleurs de conclure ou non un contrat de bail au seul motif de la situation du candidat locataire au regard du pacte ; qu'une telle collecte d'informations, à supposer même qu'elle paraisse loyale au sens de l'article 25 de la loi du 6 janvier 1978, n'est pas pertinente et paraît de nature à provoquer des discriminations entre locataires ; qu'ainsi, les dispositions de l'article 14 de la loi relative au pacte civil de solidarité qui ont pour objet de conférer un droit au transfert de bail au partenaire, en cas de décès ou de départ du locataire, pourraient être méconnues ou contournées dès lors que le bailleur, disposant d'une information sur la situation du candidat locataire, pourrait être tenté de ne pas accorder un contrat de bail à un candidat engagé dans les liens du pacte ; qu'il y a lieu pour la Commission de faire une réserve sur ce point ;

Considérant, en revanche, que l'accès des syndics de co-propriétés pour le recouvrement des créances du syndic à l'encontre d'un co-propriétaire ne paraît pas porter, compte tenu des effets juridiques du pacte, d'atteintes excessives à la vie privée des partenaires ; que, de même, l'accès, que le projet de décret envisage, d'une personne justifiant qu'elle va se marier aux informations concernant son futur époux ou épouse n'appelle pas d'observation ; qu'enfin, l'accès d'un tiers aux informations concernant son concubin ou sa concubine peut être admis, sous la réserve que ce tiers soit en mesure de rapporter la preuve de sa qualité de concubin de la personne concernée ;

Sur la délivrance d'attestation d'engagement dans les liens du pacte ou d'attestation de non engagement dans les liens d'un pacte

Considérant qu'il résulte de l'article 2 du projet de décret que les registres pourront être utilisés pour établir des attestations d'engagement dans les liens d'un pacte civil de solidarité ou des attestations selon lesquelles les personnes concernées ne sont pas engagées dans les liens d'un pacte ;

Considérant, s'agissant des attestations d'engagement dans les liens d'un pacte, que de telles attestations devront être produites, dans certaines circonstances, par les partenaires qui souhaiteront bénéficier d'un droit ou d'un avantage attaché au pacte ; que tel sera notamment le cas, à l'égard de l'employeur, pour pouvoir bénéficier des dispositions prévues par le code du travail relatives au droit pour les partenaires de prendre un congé simultané, ou au droit à un congé de deux jours lors du décès du partenaire (articles L 223-7, L 226-1 -4e alinéa et L 784-1), et, s'agissant des fonctionnaires, des dispositions statutaires relatives aux fonctions publiques en matière de rapprochement de conjoints (article 13 de la loi) ; que tel sera également le cas à l'égard du bailleur en matière de continuation du contrat de location en

cas d'abandon du domicile par un des partenaires, ou de transfert du contrat en cas de décès ; que tel sera encore le cas en matière d'affiliation à la sécurité sociale dans l'hypothèse d'une demande de rattachement du partenaire présentée sur le fondement de l'article L. 161-14 modifié du code de la sécurité sociale et, de manière plus générale, dans toutes les hypothèses dans lesquelles les partenaires liés par un pacte souhaiteront bénéficier d'un avantage attaché à sa conclusion ;

Considérant, en revanche, que la délivrance d'attestations selon lesquelles une personne n'est pas engagée dans les liens d'un pacte civil de solidarité soulève une difficulté de principe ; qu'en effet, l'existence d'une telle attestation revient à faire peser sur toute personne, et notamment des personnes célibataires ou des personnes mariées, une présomption d'être dans les liens d'un pacte, présomption qui devrait être combattue par la production de ladite attestation ; qu'une telle présomption ne saurait peser sur les personnes sans porter une atteinte excessive à leur vie privée, à leur liberté et à leur tranquillité ; qu'en outre, la possibilité que de telles attestations puissent être délivrées pourrait conduire à de nombreuses dérives en permettant à certaines personnes ou organismes de l'exiger pour des motifs illégitimes et de nature à créer des discriminations injustifiées entre personnes célibataires, partenaires d'un pacte ou personnes mariées ; qu'ainsi, il ne serait pas légitime, notamment, qu'un employeur exige la production d'un telle attestation lors d'une candidature à l'embauche, ni un bailleur lors de la conclusion d'un contrat de bail locatif ;

Considérant, de surcroît, que si l'article 515-3 nouveau du code civil exige des partenaires souhaitant se lier par un pacte la production d'une telle attestation, la mise en place d'un réseau informatique entre les greffes des tribunaux d'instance pourrait, dans le souci de simplifier les formalités administratives pesant sur les futurs partenaires, permettre au greffe du tribunal qui reçoit la déclaration de vérifier aisément cette information par la voie informatique en interrogeant directement le greffe du tribunal d'instance du lieu de naissance de chacun des partenaires ce qui dispenserait les futurs partenaires d'avoir à produire une telle attestation ;

Considérant dès lors que l'ensemble de ces observations conduit à émettre une réserve de principe sur les attestations de non engagement dans les liens d'un pacte qui, en tout état de cause, ne devraient être délivrées dans aucune autre situation que celle visée par l'article 513-3 nouveau du code civil ;

Considérant que le droit de s'opposer à la mise en œuvre du traitement informatique des informations portées sur le registre est exclu ; que les personnes pourront exercer leur droit d'accès auprès de chacun des greffes qui tient registre d'informations les concernant ;

Considérant que le projet de décret prévoit dans son article 10 que toute mise en œuvre de l'informatisation des registres devra faire l'objet d'une déclaration de conformité au présent décret précisant les mesures de sécurité et de confidentialité, tant physiques que logiques, adoptées ; que, compte-tenu de la précision des règles qui entourent le fonctionnement de ces registres et des mesures de sécurité décrites dans la demande d'avis dont la Commission est saisie, il y a lieu de tenir de tenir pour inutile l'accomplissement de ces formalités par chacun des tribunaux d'instance, par chacun des postes diplomatiques ou consulaires et par le tribunal de grande instance de Paris, le traitement mis en œuvre devant être considéré comme un modèle natio-

nal ; que, dans ces conditions, il y a lieu de supprimer l'article 10 du projet de décret ;

Sur le projet de décret portant application des dispositions de l'article 31 — alinéa 3

Considérant que le Gouvernement a saisi la Commission d'un projet de décret pris en application des dispositions de l'article 31 — alinéa 3 de la loi du 6 janvier 1978 ; que ce projet de décret a pour objet d'autoriser certaines personnes, autorités, services ou organismes à enregistrer des données qui, dans la mesure où elles sont susceptibles de révéler indirectement le sexe des partenaires d'un pacte civil de solidarité, et partant leurs mœurs, relèvent des catégories de données dont le traitement est, par principe, interdit, sauf consentement exprès des personnes ;

Considérant qu'il est d'intérêt public que les registres institués par la loi puissent être mis en œuvre ;

Considérant, en outre, qu'il est d'intérêt public que les services et organismes qui pourront avoir accès aux informations que ces registres comportent, dans les limites et aux conditions précisées par l'article 5 du décret relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à l'information, la modification et la dissolution du pacte civil de solidarité et sous les réserves exprimées ci-dessus, puissent enregistrer et conserver ces informations dans un fichier dès lors qu'il serait mis en œuvre dans le cadre de l'exercice de leurs missions légales et dans le respect des dispositions de la loi du 6 janvier 1978 ;

Considérant qu'il en est de même pour les services et organismes auxquels les partenaires d'un pacte auraient communiqué ces informations pour faire valoir les droits ou avantages qui s'attachent à la conclusion d'un pacte civil de solidarité ;

Considérant que ces dispositions n'ont d'autre objet que de dispenser les organismes qui pourront régulièrement conserver dans un fichier des informations relatives à des personnes liées par un pacte, dès lors que de telles informations seront considérées comme adéquates, pertinentes et non excessives au regard de la finalité des fichiers en cause, d'avoir à recueillir le consentement exprès des personnes ;

Considérant en outre qu'il est interdit de sélectionner une catégorie particulière de personnes à partir de ces informations ou de procéder à des tris permettant de distinguer les couples homosexuels des autres ;

Considérant que tel qu'il est rédigé, et sous les réserves exprimées par la Commission sur l'article 5 du décret « relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité et autorisant la création à cet effet d'un traitement automatisé des registres mis en œuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris et par les agents diplomatiques et consulaires français » auquel l'article 2 de ce décret renvoie, ce texte n'appelle pas d'observations particulières de la Commission ;

Sur le projet de décret relatif à la déclaration, à la modification et à la dissolution du pacte civil de solidarité

Considérant que pour les motifs ci-dessus exposés, il n'y a pas lieu de prévoir la délivrance d'attestation selon laquelle une personne n'est pas engagée dans les liens d'un pacte civil de solidarité ;

Emet

1 — **Un avis favorable** sur le projet de décret relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité et autorisant la création à cet effet d'un traitement automatisé des registres mis en œuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris et par les agents diplomatiques et consulaires français, **sous les réserves suivantes** :
— l'article 2 -3° devrait ainsi rédigé : « l'établissement des attestations prévues par l'article 515-3 du code civil, exclusivement au profit des partenaires souhaitant conclure un pacte civil de solidarité, ainsi que l'établissement des attestations d'engagement dans les liens d'un pacte civil de solidarité »,
— à l'article 5-I, premier alinéa, les mots « des informations visées aux 1°, 2°, 3°, 5°, 6° et 7° du premier alinéa de l'article 3 » devraient être remplacés par les mots « des informations visées aux 1°, 2°, 3°, 5° et 7° du premier alinéa de l'article 3, accompagnées le cas échéant de l'indication de la nature de l'acte ou du fait juridique générateur de la dissolution du pacte, exclusivement sous la forme suivante : » décès « ou » autre cause de dissolution « . »
— à l'article 5-I, le 10° est supprimé,
— à l'article 5-II, les 1°, 2°, 3° sont supprimés,
— l'article 10 est supprimé.

2 — **Un avis conforme** au projet de décret portant application des dispositions du 3e alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux registres mis en œuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris, et par les agents diplomatiques et consulaires français, aux fins d'assurer le traitement et la conservation des informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité sous réserve, à l'article 2, que les mots « ainsi qu'au 1° à 4° du II de l'article 5 » soient remplacés par les mots « ainsi qu'au 4° du II de l'article 5 ».

3 — **Un avis favorable** au projet de décret pris en application de la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité et relatif à la déclaration, à la modification et la dissolution du pacte civil de solidarité sous les réserves suivantes :
— à l'article 2, le quatrième alinéa devrait être ainsi rédigé : « Le greffe du tribunal de grande instance du lieu de naissance ou, en cas de naissance à l'étranger, du tribunal de grande instance de Paris, délivre à la personne concernée l'attestation qui doit être produite au greffe du tribunal d'instance lors de la déclaration conjointe de conclusion d'un pacte »,
— à l'article 2, cinquième alinéa, la référence faite aux attestations selon lesquelles les personnes ne sont pas liées par un pacte civil de solidarité est supprimée, ainsi que la référence faite aux personnes visées au 10° du I et aux organismes ou personnes visées aux 1°, 2° et 3° du II,

— à l'article 2, sixième alinéa, les mots « personnes mentionnées aux 1° à 6° du II dudit article » sont remplacés par les mots « personnes mentionnées aux 4°, 5° et 6° du II dudit article ».

III. TROIS ACTIONS POUR DIFFUSER LA CULTURE INFORMATIQUE ET LIBERTÉS

A. La préparation d'un code de déontologie du commerce et de la distribution

La CNIL a été consultée par la fédération du commerce et de la distribution (FCD) à propos de l'élaboration d'un code de déontologie relatif à la protection des données personnelles des consommateurs dans les enseignes des entreprises du commerce et de la distribution. La Commission a jugé très utile cette initiative, car ce code viserait à encadrer les stratégies de fidélisation de la clientèle qui supposent une analyse de plus en plus fine des attentes ou des achats du consommateur.

Ce code s'inscrit dans la lignée des deux codes de déontologie précédemment adoptés dans le secteur du marketing direct après concertation avec la CNIL. D'une part, le code de déontologie des professionnels du marketing direct, élaboré en décembre 1993 sous l'égide de l'Union française du marketing direct (cf 14e rapport d'activité, p. 27). D'autre part, le code de déontologie sur les bases de données comportementales, élaboré en novembre 1998 sous l'égide du syndicat des entreprises de vente par correspondance et à distance, et grâce auquel les deux principaux opérateurs de mégabases de données comportementales se sont engagés à respecter les principales règles ressortant de la recommandation de la CNIL n° 97-012 du 18 février 1997 (cf 18e rapport d'activité, p. 53).

Dès 1995, la CNIL avait statué sur une application destinée à des supermarchés, qui, dans le but de sécuriser les paiements par chèque, consistait à ne valider l'encaissement qu'après vérification du fichier des impayés de chèques du magasin et, le cas échéant, interrogation du fichier national des chèques irréguliers géré par la Banque de France. Au-delà de cet objectif, ce procédé permettait aussi de repérer les bons clients et de les fidéliser en accélérant leur passage en caisse (cf 16e rapport d'activité, p. 131).

Depuis lors, la Commission a pu examiner, au fil des déclarations, d'autres systèmes de collecte et d'exploitation d'informations en vue de la fidélisation de la clientèle (attribution de points en fonction des achats, segmentation au regard de la nature du produit acheté, du montant et de la fréquence des achats, carte de fidélité en contrepartie d'informations sur le foyer et de bons d'achat...). En tout état de cause, il ne fait pas de doute que le cumul des informations figurant sur le ticket de caisse et celles obtenues via une carte de fidélité permettent d'établir un profil précis du consommateur (« panier du consommateur »). C'est pour faire face à ces nouveaux enjeux, dans des conditions de plus grande loyauté et de meilleure information

des consommateurs, que les professionnels ont souhaité rédiger un code de déontologie.

Au total, il faut retenir que ce code s'appliquerait dès lors que des données personnelles sont collectées, que ce soit directement auprès de la personne concernée ou auprès de tiers, que la collecte résulte d'un acte de volonté (personne remplissant un questionnaire ou un coupon) ou qu'elle soit opérée à l'occasion d'un passage en caisse, enfin, qu'elle soit effectuée dans le magasin ou en ligne. Il est prévu que les mentions d'information sur les droits garantis par la loi « informatique et libertés » soient systématiquement portées sur le support de collecte, et à défaut dans le premier document adressé au client. S'agissant de la collecte de données à partir de sites internet, la Commission a pris note avec grande satisfaction que les personnes seraient en mesure d'exercer directement en ligne leur droit d'opposition à l'exploitation de leurs données à des fins commerciales, d'une part, et à la cession de leurs coordonnées à des tiers, d'autre part. Il s'agit là d'un engagement déontologique conforme aux recommandations de la CNIL et aux prescriptions de la directive européenne 95/46.

Il reste à cette organisation professionnelle, après l'important travail de concertation qui a eu lieu en liaison avec la CNIL, à faire connaître ce code aux professionnels concernés et à veiller à sa bonne application.

B. L'espace juniors du site internet de la CNIL

Ouvert le 6 janvier 1998, le site internet de la CNIL est, sous de nombreux aspects, comparable à d'autres sites institutionnels. Accessible à l'adresse http://www.cnil.fr, le site contient de nombreuses informations concernant la loi, les droits des personnes, les obligations des détenteurs de fichiers, les modalités de déclaration des traitements informatiques ou encore de nombreux textes officiels et des guides thématiques. Pourtant ce site se singularise en dévoilant aux internautes comment ils laissent, à leur insu, des traces sur internet (cf 18^{e} rapport d'activité, annexe 6 et infra). En effet, chaque internaute se voit restituer en direct l'intégralité de son parcours, démonstration interactive que les déplacements sur le réseau sont repérables (cf 18^{e} rapport d'activité, p. 343).

Début 2000, la CNIL a enrichi son site d'un espace destiné aux juniors (8-12 ans). L'objectif de cette nouvelle rubrique est de sensibiliser les jeunes aux questions de protection des données, à l'heure où ils sont tous conduits à faire l'apprentissage des nouvelles technologies, en particulier de l'internet. Au surplus, la CNIL a pu constater d'importantes pratiques de collecte d'informations personnelles de la part des sites internet pour les jeunes (inscription en ligne préalablement à la navigation, dates anniversaires, jeux, adhésions à des clubs etc).

L'espace juniors oriente vers 4 grandes rubriques :
— « Tes traces » montre au jeune internaute comment il est « pisté » sur internet,
— « La CNIL » donne des informations sur le rôle et les missions de la Commission.
— « Tes droits » explique les droits fondamentaux garantis par la loi « Informatique et Libertés » et la CNIL,

— Un quizz permet de découvrir en quelques clics si l'on connaît ses droits sur internet.

La navigation peut être complétée d'une visite sur un webdico qui explique simplement les termes techniques employés sur le site.

Le site internet juniors de la CNIL a été conçu pour constituer un matériel pédagogique utilisable dans les établissements scolaires, dans le cadre d'un cours d'éducation civique ou lors d'événements tels que la « Semaine des initiatives citoyennes » ou bien la fête de l'internet. La CNIL souhaiterait en effet vivement que les établissements d'enseignement, dont il a été souligné qu'ils devaient constituer des lieux d'apprentissage de la citoyenneté, puissent devenir des relais dans la promotion du droit de chacun à voir ses données et sa vie privée protégées.

C. Le Cédérom « Internet au sud »

Dans le cadre de sa mission générale de sensibilisation à la loi « Informatique et Libertés », la CNIL a apporté sa contribution à un cédérom intitulé « Internet au sud ». Ce cédérom produit par l'UNESCO, et réalisé par une équipe de l'Institut des Nations unies pour la formation et la recherche (UNITAR) et de l'Institut de recherche pour le développement (IRD) a vocation à être diffusé dans les pays en voie de développement, afin de renforcer leur expertise technique et leur maîtrise des technologies de l'information. Destiné à des populations qui risquent d'être plus encore marginalisées par un accès limité aux nouveaux moyens de communication, ce cédérom constitue un support de formation et une riche documentation sur internet et ses applications, et une étape préalable à la mise en œuvre d'un site web. La CNIL a été très heureuse d'être sollicitée dans le cadre de cette initiative destinée à réduire le « fossé numérique » entre le Nord et le Sud.

LE NIR, UN NUMÉRO PAS COMME LES AUTRES

Communément appelé « numéro de sécurité sociale », le NIR, ou numéro d'inscription au répertoire national d'identification des personnes physiques, constitue sans doute aujourd'hui, avec le numéro de téléphone, le digicode de la porte d'entrée et les codes secrets du téléphone portable et de la carte bancaire, un numéro dont chacun se souvient et dont l'usage est courant. Ce numéro est, en effet, porté sur la carte d'assuré social, sur les feuilles de soins, sur les décomptes de prestations. En revanche, il n'apparaît ni sur la carte d'identité, ni sur le passeport, ni sur le permis de conduire, ni sur la déclaration de revenus, ni sur les relevés bancaires, ni encore sur le livret scolaire.

Pourquoi ? Parce que ce n'est pas un numéro comme un autre.

En raison de ses origines et de sa composition, d'abord. Construit sous l'égide de l'INSEE et certifié par lui à partir d'éléments d'état civil transmis par les mairies (sexe, année et mois de naissance, département et commune de naissance, numéro d'ordre du registre d'état civil), le NIR constitue un identifiant fiable et stable, conçu pour rester immuable la vie durant. Cependant, créé sous le régime de Vichy pour classer les fichiers administratifs et établir des statistiques démographiques, le NIR a été aussitôt utilisé pour distinguer « juifs » et « non-juifs » selon les critères des autorités antisémites de l'époque, la première position du numéro relative au sexe des personnes ayant été complétée sur cette base. Cette mémoire restera attachée au NIR.

Il est vrai que la structure de ce numéro pouvait faciliter de telles discriminations. De fait, le NIR est le reflet, sous forme numérique, de l'identité de chacun. Dès lors, la tentation est toujours grande pour les gestionnaires, plutôt que de désigner les individus par leur état civil complet, de faire appel de préférence à des numéros qui facilitent l'accès aux fichiers et les interconnexions entre fichiers. En outre, les

caractéristiques mêmes de cet identifiant — qui est particulièrement signifiant à la différence de la plupart des identifiants utilisés à l'étranger — induisent un risque de sélections immédiates de catégories entières de population sur la base de certains des champs composant le numéro, notamment ceux qui correspondent au département ou pays de naissance et qui permettent ainsi de classer d'emblée les personnes nées à l'étranger ou outre-mer. Ainsi, une utilisation non-contrôlée du NIR serait susceptible d'entraîner des traitements non personnalisés des situations individuelles, voire l'engagement d'actions selon des critères discriminants et non légitimes.

Cela est si vrai que le gouvernement a saisi la CNIL d'un projet de décret destiné à permettre aux personnes nées en Algérie avant le 3 juillet 1962, et déjà immatriculées, de demander la modification de leur NIR, afin de substituer au code 99, affecté à toutes les personnes nées à l'étranger, un nouveau code (de 91 à 94) pour identifier leur lieu de naissance. Seul le caractère signifiant de ce numéro et le risque de discrimination entre Français et étrangers pouvait justifier une telle initiative.

On comprend, dans ces conditions, que l'article 18 de la loi « informatique et libertés » ait disposé que « l'utilisation du répertoire national d'identification des personnes physiques en vue d'effectuer des traitements nominatifs est autorisé par décret en Conseil d'Etat pris après avis de la Commission » et que la CNIL ait toujours donné sa pleine portée à cette disposition législative en constatant la relation étroite qui existe entre le numéro de sécurité sociale et le NIR (cf 2e rapport d'activité 1980-1981 p. 26). Elle a ainsi estimé que l'utilisation du numéro de sécurité sociale équivalait à l'utilisation du RNIPP et que la procédure prévue par l'article 18 de la loi devait s'appliquer dès lors que le numéro de sécurité sociale était directement collecté auprès de la personne concernée et conservé dans un fichier, même s'il n'y avait aucune utilisation du répertoire tenu par l'INSEE.

Autrement dit, il était clair, au départ, que la procédure prévue par l'article 18 avait pour objet de restreindre le recours au NIR.

Aussi était-il prévisible que l'adoption, à la fin de l'année 1998, d'un amendement à la loi de finances pour 1999 autorisant les administrations financières à collecter, conserver et transmettre le NIR ait suscité, à nouveau, un débat public. La CNIL a rappelé dans son 19e rapport d'activité (p. 39 à 47) les éléments de doctrine qu'elle avait dégagés sur la base de la loi du 6 janvier 1978 en cette matière qui met en cause des principes essentiels de cette loi fondatrice, tels que le principe de finalité, les interconnexions entre fichiers, et le cantonnement du NIR dans ce qu'il est convenu d'appeler par commodité la « sphère sociale ».

La CNIL n'avait pas été consultée à l'occasion du vote de l'amendement qui allait aboutir à l'article 107 de la loi des finances pour 1999 ; d'où un important travail d'instruction en 1999, lorsqu'elle a été saisie, conformément à la volonté du législateur, des textes d'application de cet article. Les avis que la Commission a rendus sur les dispositifs qui lui étaient soumis portent la marque de convictions fermes mais qui tiennent compte de l'évolution du contexte juridique.

Sans doute l'usage du NIR, jusqu'alors cantonné au domaine social, a-t-il été étendu, par la loi, au domaine fiscal. Cependant, loin de renoncer aux éléments de

doctrine qu'elle avait dégagés depuis 20 ans, la Commission a limité l'utilisation du NIR par les administrations financières à une fonction précise de sécurisation de l'identifiant fiscal. Ce faisant, fidèle aux origines, la CNIL a souhaité éviter que le NIR ne devienne un identifiant généraliste qui puisse se diffuser d'un fichier à un autre, ouvrant la voie à de nouvelles interconnexions.

I. LE NIR, UN IDENTIFIANT FINALISÉ ET CANTONNÉ AU DOMAINE SOCIAL

La conviction de la CNIL, forgée à la lumière des débats suscités par le projet SAFARI et qui allaient aboutir à l'adoption de la loi du 6 janvier 1978, est, depuis l'origine, qu'il faut éviter toute conception « universaliste » du NIR, qui en ferait, pas à pas, un numéro identifiant utilisé dans tous les fichiers sans égard pour leurs finalités propres. C'est dans cet esprit que la Commission a d'ailleurs proscrit l'usage du terme « numéro national d'identité » au profit de l'expression « numéro d'inscription au répertoire national d'identification des personnes physiques ».

A. Le confinement du NIR au domaine social

La position de principe de la CNIL n'excluait pas tout pragmatisme. Ainsi, la Commission a dû constater, dans sa recommandation du 23 novembre 1983 relative à la consultation du répertoire national d'identification des personnes physiques et l'utilisation du NIR, que « le NIR a été utilisé d'emblée comme identifiant par la plupart des organismes intervenant dans le secteur de la sécurité sociale, cette utilisation marquant une extension de la finalité du numéro, aujourd'hui enregistré dans tous les traitements automatisés d'informations nominatives concernant des opérations en relation avec la sécurité sociale » et « que cette extension de finalité ne peut être remise en cause, sauf à entraîner de graves perturbations dans le fonctionnement du régime de protection sociale ».

Ainsi le décret du 3 avril 1985, pris après avis favorable de la CNIL, a autorisé, pour l'exercice de leurs missions, l'ensemble des organismes de protection sociale chargés de la gestion des régimes obligatoires de sécurité sociale (assurance maladie, assurance vieillesse, allocations familiales, recouvrement des cotisations sociales) à recourir au répertoire et à utiliser le NIR dans leurs fichiers.

Vigilante et soucieuse de cantonner le NIR au domaine social, la Commission a, dès l'origine, entrepris de convaincre les administrations qui souhaitaient recourir au NIR ou qui l'utilisaient sans y être autorisées, d'y renoncer et de se doter d'un numéro spécifique. Tel a été le sens, et le succès, de l'action entreprise à l'égard du ministère de l'éducation nationale qui a finalement, en 1992, substitué le NUMEN au NIR, comme identifiant principal, dans ses fichiers de gestion interne.

Il convient cependant de reconnaître que le « domaine social » s'est considérablement élargi et qu'il n'est plus cantonné au seul secteur de la sécurité sociale,

comme la Commission le constatait déjà dans son 7e rapport d'activité pour 1986 : « *Le NIR se diffuse en effet, selon des filières qui partent toutes de la sécurité sociale et contaminent progressivement tout le champ des rapports entre les employeurs et les salariés d'une part, et celui de la santé d'autre part. En partant du secteur de la protection sociale qui a été étendue à des catégories de travailleurs de plus en plus nombreuses et pour gagner finalement toute la population (cotisations des employeurs), le NIR est employé pour la gestion de la paie (norme simplifiée), les traitements concernant les avantages sociaux annexes accordés par les employeurs (restaurant d'entreprise) puis de fil en aiguille, la gestion des carrières, de la formation permanente, des horaires, puis les activités du service médical des entreprises, des comités d'entreprises. De la sécurité sociale au sens strict, on glisse à la gestion des malades dans les hôpitaux (admissions), aux traitements de recherche épidémiologique, à la gestion des laboratoires d'analyse, à la gestion des pharmacies (tiers payant). Dans tous ces secteurs, il est peu probable que l'on puisse raisonnablement empêcher le NIR de se généraliser.* »

Cette prévision s'est réalisée. Sous l'effet des lois sociales successives, le cercle des partenaires « naturels » de la sécurité sociale s'est en effet progressivement élargi. Qu'il s'agisse de payer des cotisations sociales, d'assurer aux chômeurs le maintien de leurs droits sociaux, de permettre la prise en charge totale ou partielle des frais de maladie, les acteurs du système de protection sociale — employeurs, ASSEDIC et ANPE, organismes d'assurance maladie complémentaires, professionnels de santé… — ont tous été conduits, au titre de leurs relations avec la sécurité sociale, à recueillir et à utiliser le numéro de sécurité sociale dans leurs fichiers. Plusieurs décrets sont alors intervenus pour autoriser de telles utilisations dont l'objet demeurait cependant cantonné à leurs relations avec les organismes de sécurité sociale.

A ce titre, outre les employeurs, les organismes de protection complémentaires, les services d'aide sociale, l'ANPE, les institutions gestionnaires du régime d'assurance chômage, les professionnels et établissements de santé ont été autorisés à utiliser le NIR dans leurs relations avec la sécurité sociale.

S'agissant des professionnels et établissements de santé, l'enregistrement du numéro de sécurité sociale dans leurs fichiers de gestion administrative et de facturation n'a été légalisé que tardivement, par un décret du 12 septembre 1996, et, conformément à la doctrine dégagée par la CNIL, pour les seuls traitements que les professionnels et établissements de santé effectuent pour leurs échanges avec les organismes de protection sociale. Les comptables publics attachés aux établissements de santé ont également été autorisés à utiliser ce numéro pour les traitements qu'ils réalisent aux fins de recouvrement de créances auprès des assurés sociaux soignés par leurs établissements. Dans un avis rendu le 9 juillet 1996 sur ce projet, la CNIL a d'ailleurs émis une forte réserve quant à l'utilisation du NIR comme numéro identifiant du patient dans la sphère médicale au motif qu'aucune justification précise et convaincante n'était apportée sur ce point.

B. Le refus de toute utilisation non finalisée du NIR

Parallèlement, et dans le souci de limiter autant qu'il était possible les usages du NIR par ceux des organismes ou administrations qui étaient autorisés à l'utiliser, la Commission a, dès 1983, fait référence à la nécessité de limiter l'utilisation du NIR comme identifiant « dès lors qu'il n'apparaît pas indispensable à la finalité du traitement ». Aussi, les décrets pris sur le fondement de l'article 18 ne se bornaient-ils plus à autoriser la consultation du RNIPP ou l'utilisation du NIR ou du numéro de sécurité sociale dans certains fichiers, mais précisaient les finalités, c'est-à-dire l'utilisation précise qui serait faite du NIR. Ainsi, dans un souci de meilleure garantie et de précaution, la CNIL a prolongé le principe de finalité d'un traitement pris dans son ensemble à celui de l'usage spécifique qui pouvait être fait d'une information particulière : le NIR.

C. Le strict encadrement des interconnexions

La doctrine du « cantonnement » du NIR a conduit la Commission à considérer que la seule nécessité d'établir une interconnexion entre fichiers ne justifiait pas, à elle seule, qu'une administration qui ne dispose pas du NIR puisse s'en doter ou encore que le NIR devienne un élément identifiant dans l'ensemble des fichiers de l'administration concernée.

En revanche, si deux administrations sont autorisées à utiliser le NIR dans leur propre fichier et à procéder entre elles à des échanges d'informations, la CNIL ne s'oppose pas à ce que les interconnexions puissent avoir lieu sur la base du NIR (cf 19e rapport d'activité, p. 42).

La position de la CNIL pourrait être ainsi résumée : au regard du principe de finalité, le problème le plus important est celui des interconnexions ; si l'interconnexion est autorisée par la loi, le NIR, qui la facilite, peut être utilisé. En revanche, l'interconnexion ne doit pas être un vecteur de transmission du NIR à une administration qui n'aurait pas été préalablement autorisée à l'utiliser.

Dans le domaine social, les rapprochements de fichiers, parce qu'ils concernent des informations couvertes par le secret, résultent tous de dispositions spécifiques votées par le Parlement et reposent donc sur des fondements juridiques non contestables, qu'il s'agisse de la loi de 1988 relative au RMI (article 21), du code du travail (articles L 124-11, L 351-21) ou du code de la sécurité sociale (article L 311-5).

Ces interconnexions ont généralement pour but de vérifier la réalité de la situation sociale des demandeurs. La Commission s'est ainsi prononcée en 1995 sur l'utilisation du NIR dans le cadre d'échanges entre les caisses d'allocations familiales et les organismes chargés de l'indemnisation du chômage (UNEDIC et ASSEDIC) et le CNASEA aux fins de vérification des droits des bénéficiaires du RMI et en particulier des ressources déclarées par ces derniers (décret du 16 juillet 1996). Elle avait auparavant autorisé les caisses d'allocations familiales à signaler aux agences locales pour l'emploi, les bénéficiaires du RMI afin que celles-ci soient en mesure de leur

proposer des mesures d'insertion. Ces échanges d'informations se sont effectués en recourant au NIR (décret du 16 octobre 1990).

Depuis un décret du 7 septembre 1992, les ASSEDIC sont également autorisées à utiliser le NIR, dans le cadre d'un traitement de rapprochement des déclarations des demandeurs d'emploi et des relevés mensuels des contrats d'entreprises de travail temporaire transmis par ces dernières aux directions départementales du travail et de l'emploi, ceci afin de vérifier notamment le contrôle de la recherche d'emploi, y compris la détection des situations de fraude.

Enfin, des échanges d'informations, toujours fondés sur le NIR, ont été organisés entre les ASSEDIC et les caisses d'assurance maladie pour établir les droits à la couverture sociale des travailleurs privés d'emploi ou des pré-retraités (avis favorable du 23 juin 1992) et contrôler les cumuls éventuels d'allocation chômage et d'indemnités journalières (avis favorable du 6 décembre 1994).

En tout état de cause, s'agissant des interconnexions de fichiers publics, qu'elles soient opérées avec ou sans le NIR, il n'y a pas d'interconnexion qui puisse être mise en œuvre à l'insu des personnes concernées ou en méconnaissance d'un secret légalement protégé, sauf si le législateur en décide autrement.

Force est cependant de constater que la tentation est forte de s'en remettre au NIR comme à un identifiant généraliste, structurant la base de données, sans égard pour sa finalité propre et au motif de plus grandes commodités administratives.

Cette tentation ne peut que renforcer l'engagement de la CNIL à préconiser l'adoption d'identifiants spécifiques. C'est sur la base de cette conviction que la Commission procède à l'examen des mesures d'application de l'article 107 de la loi de finances pour 1999.

II. LE NIR, UN OUTIL DE SÉCURISATION DE L'IDENTIFIANT FISCAL

C'est — on l'a dit — à la suite du vote d'un amendement au projet de loi de finances pour 1999, que les administrations financières ont été autorisées à utiliser le NIR (cf 19e rapport d'activité, p. 39). Cet élément factuel est important à rappeler dans la mesure où il a été trop souvent dit et écrit que cette disposition avait été prise par la CNIL ou après avoir recueilli son accord.

L'article 107 de la loi de finances pour 1999, issu de cet amendement, autorise désormais la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects :

— à collecter, conserver et échanger entre elles les numéros d'inscription au répertoire national d'identification des personnes physiques pour les utiliser exclusivement dans les traitements des données relatives à l'assiette, au contrôle et au

recouvrement de tous impôts, droits, taxes, redevances ou amendes et aux seules fins d'accomplissement de ces missions (article L. 287 nouveau du livre des procédures fiscales — LPF),

— à utiliser ce numéro pour les demandes, échanges et traitements nécessaires à la communication, aux organismes chargés de la gestion d'un régime obligatoire de sécurité sociale et aux institutions de retraite complémentaire, des informations nominatives nécessaires à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions ainsi qu'à leur recouvrement (article L. 152 modifié du LPF).

En outre, le nouvel article législatif prévoit que, lorsqu'est exercé le droit de communication prévu à l'article L. 81 du LPF, les informations nominatives communiquées, sur tout type de support, par les personnes ou organismes autorisés à utiliser le NIR à l'égard desquelles ce droit peut légalement s'exercer, mentionnent le NIR (article L. 81 A nouveau du LPF)

La présentation de l'amendement avait fait naître des craintes. La CNIL a continué, à la place qui est la sienne, à défendre ses convictions, qui l'ont conduite, en s'appuyant sur les garanties fixées tant par le législateur que par le juge constitutionnel, à encadrer le plus précisément possible les conditions d'utilisation du NIR par les administrations fiscales.

A. L'encadrement législatif

Le législateur a assorti de plusieurs garanties la nouvelle autorisation d'utiliser le NIR.

En premier lieu, l'article 107 prévoit, dans le cas où la mise en œuvre du droit de communication s'avérerait susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi du 6 janvier 1978, la faculté pour la CNIL d'enjoindre l'autorité administrative de prendre sans délai des mesures de sécurité pouvant aller jusqu'à la « destruction des supports d'informations qui ont été constitués à partir d'un NIR ».

Ce faisant, le Législateur a souhaité élargir encore, dans ce cas particulier, les cas d'application de l'article 21 de la loi du 6 janvier 1978 qui prévoit, au titre des rares mesures réglementaires pouvant être prises par la CNIL, la possibilité pour elle, dans le seul cas de circonstances exceptionnelles, de prescrire des « mesures de sécurité pouvant aller jusqu'à la destruction des supports d'informations ».

Sur la base de cette disposition, la Commission a déjà été amenée à souhaiter, à l'occasion de la création de certains fichiers, que figurent, au titre de leurs caractéristiques et compte-tenu de leur sensibilité particulière, les modalités pratiques de leur destruction en cas de circonstances exceptionnelles. Tel a été notamment le cas lors de l'examen du Répertoire national inter-régimes des bénéficiaires de l'assurance maladie (RNIAM) dont le principe résulte d'une ordonnance du

24 avril 1996 et dont les modalités ont été fixées par un décret du 10 septembre 1996 et un arrêté du 22 octobre 1996, pris après avis favorable de la CNIL (cf 17e rapport d'activité, p 261). Le RNIAM, géré par la Caisse nationale d'assurance vieillesse a vocation à contenir le NIR, les identités, les date et lieu de naissance de l'ensemble des assurés sociaux et ayant droits ainsi que l'identifiant de l'organisme qui leur sert les prestations d'assurance maladie.

S'agissant de l'article 107, les précautions prises par le Législateur ont une portée plus large dans la mesure où la possibilité pour la CNIL de prendre des mesures de sécurité n'y est pas conditionnée à la survenance de « circonstances exceptionnelles ». En effet, les « atteintes graves et immédiates aux droits et libertés » incluent aussi, par exemple, les cas de désordre informatique.

Cette disposition constitue un précédent qui souligne à la fois la spécificité du NIR et, du fait de son élargissement par rapport à l'article 21 de la loi du 6 janvier 1978, le caractère de « garantie fondamentale » en matière de libertés publiques que revêt le pouvoir d'injonction reconnu à la CNIL.

En outre, l'article 107 de la loi de finances pour 1999 alourdit les sanctions pénales encourues en cas de violation du secret professionnel ou d'utilisation à d'autres fins des informations collectées par les administrations financières. La seule information nouvelle pouvant, désormais, être détenue par l'administration fiscale étant le NIR, cette répression accrue ne peut que renforcer la conviction que ce numéro n'est pas un numéro comme les autres.

Enfin, la loi renvoyait à un décret en Conseil d'Etat pris après avis de la CNIL la détermination des modalités d'application du dispositif d'ensemble.

B. Les barrières constitutionnelles

Ce sont les risques inhérents à l'utilisation du NIR qui ont également conduit le Conseil constitutionnel, lors de l'examen de la constitutionnalité de l'article 107, à n'admettre cette disposition, dans sa décision DC du 29 décembre 1998, qu'au prix de réserves d'interprétation concernant sa portée et sa mise en œuvre.

En premier lieu, il résulte de la décision du Conseil Constitutionnel que la portée de l'article 107 est restreinte à des finalités définies de manière précise et limitative. En effet, selon le Conseil, la loi « se borne » à permettre aux administrations financières concernées d'utiliser le NIR « en vue d'éviter les erreurs d'identité et de vérifier les adresses des personnes », dans le cadre de leurs missions respectives, ainsi qu'à l'occasion des transferts autorisés de données, soit au bénéfice des administrations concernées dans le cas des transferts de données opérés en application de l'article L. 81 A du LPF, notamment lors de l'exercice du droit de communication, soit au bénéfice des organismes de protection sociale visés à l'article L. 152 du LPF. En outre, s'agissant de la mention du NIR à l'occasion des communications au profit des organismes de protection sociale, « ces communications doivent être strictement nécessaires et exclusivement destinées à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de

l'assiette et du montant des cotisations et contributions, ainsi qu'à leur recouvrement ». Ainsi se trouve pleinement confirmée l'idée que toute utilisation du NIR doit être précisément et strictement finalisée.

En second lieu, selon le Conseil, la constitutionnalité du dispositif est établie sous réserve de quatre garanties dont est assortie la mise en œuvre de l'article 107 de la loi de finances susvisée, à savoir le respect du secret professionnel, la pleine application des dispositions protectrices de la liberté individuelle et de la vie privée établies par la législation relative à l'informatique, aux fichiers et aux libertés, l'interdiction d'utiliser le NIR pour la constitution de fichiers nominatifs sans rapport direct avec les opérations incombant aux administrations financières et sociales ou pour la mise en œuvre de tout nouveau transfert d'informations nominatives entre administrations et, enfin, l'existence d'une faculté d'intervenir conférée à la CNIL « lorsque la mise en œuvre du droit de communication prévu aux articles L. 81 A et L. 152 s'avère susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi n° 78-17 du 6 janvier 1978 ». Ainsi l'autorité prééminente de la loi du 6 janvier 1978 et de la CNIL, son bras séculier, se trouve réaffirmée.

C. La limitation de la finalité du NIR par la CNIL

Le ministère de l'Economie, des finances et de l'industrie a soumis à l'examen de la Commission un projet de décret en Conseil d'Etat, conformément à la volonté du Législateur rappelé par le Conseil constitutionnel. Ce texte complète la partie réglementaire du livre des procédures fiscales, précise les conditions et les objectifs de la collecte du NIR par les administrations financières et les modalités des communications d'informations fiscales aux organismes chargés de la gestion d'un régime obligatoire de sécurité sociale et aux institutions de retraite complémentaire prévues à l'article L. 152 du LPF.

Ce projet résulte, tout comme la lettre d'engagement des ministres qui l'accompagne, d'un long travail d'instruction mené par la Commission, en concertation avec le ministre chargé du Budget. Au cours des discussions, la Commission a mis en évidence que l'article 107 de la loi de finances pour 1999 ne devait et ne pouvait être interprété comme autorisant les administrations financières à faire du NIR un identifiant fiscal. Au contraire, l'habilitation législative, interprétée à la lumière de la décision constitutionnelle, devait conduire à limiter l'usage du NIR à fiabiliser les éléments d'identification détenus par l'administration fiscale sur les assujettis, sans que le NIR soit présent dans l'ensemble des fichiers locaux de l'administration fiscale. En précisant ceci, la Commission entendait, comme elle l'avait fait précédemment pour d'autres administrations, inciter l'administration fiscale à généraliser l'utilisation d'un numéro identifiant spécifique (le SPI [« Simplification des procédures d'identification »]) dont elle disposait d'ailleurs déjà, plutôt que d'avoir recours, par commodité, au NIR.

Aussi bien, le schéma d'ensemble proposé par le ministère à l'issue des longues discussions avec la Commission reposait-il sur la mise en place d'une table de correspondance faisant le lien entre le NIR et le SPI de sorte que seul ce dernier

numéro, propre à l'administration fiscale, identifie les contribuables et soit, à l'avenir, utilisé dans les relations entre l'administration fiscale et les contribuables. C'est notamment le numéro SPI, et non le NIR qui sera porté sur les déclarations fiscales pré-imprimées, et à terme sur les « déclarations fiscales express ».

Le NIR sera collecté par l'administration fiscale auprès de l'INSEE et, de manière exceptionnelle, auprès des personnes physiques tenues de souscrire une déclaration d'impôt sur le revenu ou redevables d'un impôt, droit, taxe, redevance, pénalité ou amende. En définitive, les seules hypothèses de recueil du NIR auprès des particuliers à avoir été retenues concernent le paiement de la taxe d'habitation et des taxes foncières établies au titre de l'année 2000, la première souscription d'une déclaration d'impôt sur le revenu et, dans le cadre de demandes de renseignement spécifique, lorsque la connaissance du NIR sera nécessaire à la vérification et à la certification de l'identité du contribuable.

Pour compléter ces garanties, les ministres ont, en outre, pris l'engagement de cantonner le NIR dans des bases nationales sécurisées et excluent sa présence dans les traitements de gestion.

A la suite, toutefois, de l'examen du texte par le Conseil d'État, le gouvernement a apporté des modifications au texte qui avait recueilli un avis favorable de la CNIL, essentiellement au sujet des finalités d'utilisation du NIR par les administrations financières. Ainsi, le décret n° 99-1047 du 14 décembre 1999 prévoit que le NIR sera utilisé non seulement pour vérifier la fiabilité des éléments d'identification des personnes physiques mais également pour l'exercice du droit de communication à l'égard des fichiers qui comportent le NIR, nécessitent que les services locaux des impôts accèdent à cet identifiant.

Cette évolution ne correspond pas à la logique développée par la Commission en ce qu'elle tend à remettre en cause l'exclusivité de la finalité d'identification du NIR et risque de porter atteinte à l'efficacité du dispositif de destruction des supports comportant le NIR.

En tout état de cause, et compte-tenu des risques réels d'erreur induits par l'utilisation exclusive de chiffres, la Commission a rappelé, dans sa délibération n° 99-033 du 24 juin 1999, que l'identité d'une personne ne saurait se réduire à un numéro matricule et a estimé que les échanges et communications d'informations appelés à comporter le NIR ne devaient pouvoir être mis en œuvre que si ce numéro était accompagné des éléments d'état civil des personnes concernées et que si l'ensemble de ces éléments était pris en compte.

L'article 1er, paragraphe II du décret du 14 décembre 1999 précise ainsi que les personnes ou organismes tenus de fournir des informations aux administrations financières en cas d'exercice du droit de communication ne devaient transmettre le NIR des personnes physiques qu'en complément des éléments d'identification de celles-ci.

De même, l'article 2, paragraphe III du décret, relatif aux demandes de renseignements présentées par les organismes sociaux au titre de l'article L 152 du LPF, précise qu'il ne peut être donné suite à une demande qu'en cas de concordance suffisante

des éléments d'identification de la personne concernée contenus dans la demande avec ceux détenus par l'administration financière à laquelle elle s'est adressée.

La liste des organismes destinataires et le détail des informations communiquées par la DGI seront, dans chaque cas, fixés dans le cadre des arrêtés interministériels prévus par le décret pour préciser les modalités d'application de chacun des traitements.

Par ailleurs, la CNIL a considéré, dans son avis du 24 juin 1999, que, pour éviter la conservation par un organisme de protection sociale d'informations financières dont il n'aurait pas dû normalement avoir à connaître par suite d'une erreur dans la constitution du fichier des demandes d'informations ou par suite d'un changement dans la situation personnelle de la personne concernée au regard de la législation sociale, les allocataires, assurés sociaux et pensionnés devraient être tenus informés de la liste des organismes destinataires, sur le fondement de l'article L. 152, d'informations nominatives les concernant. Une telle communication devait être de nature à mettre les personnes concernées en mesure d'exercer, le cas échéant, le droit de rectification ouvert par l'article 36 de la loi du 6 janvier 1978. Le souhait de la CNIL de voir le projet de décret complété en ce sens n'a pas été suivi par le Gouvernement.

Enfin, la Commission a considéré — et le gouvernement s'est finalement rangé à cet avis — que l'entrée en vigueur de l'ensemble du dispositif devait être conditionné à la publication d'un second texte réglementaire, destiné à préciser la nature des dispositifs de sécurité que les administrations financières doivent mettre en œuvre et à aménager les modalités procédurales de droit commun pour le contrôle et la mise en œuvre des mesures envisagées dans le cas de l'application des dispositions de l'article L. 288 du livre des procédures fiscales.

Ce texte, à la rédaction duquel devait être associé le ministère de la Justice, était destiné, dans l'esprit de la Commission, à définir les conditions devant être remplies pour rendre opératoire le mécanisme prévu par cet article, qui dispose qu'en cas de menace d'atteinte grave et immédiate aux droits et libertés, des mesures parfois importantes peuvent être prises « sans délai » sur injonction de la CNIL.

L'importance accordée par le législateur à l'article L. 288, introduit en fin de procédure parlementaire afin d'apaiser les inquiétudes, est, en effet, incontestable. En outre, le Conseil constitutionnel a accordé un rôle pivot à ce dispositif en estimant qu'il s'agissait là d'une garantie essentielle et il l'a fait figurer pour cette raison au nombre des réserves d'interprétation contenues dans sa décision.

C'est dans ces conditions qu'un second texte réglementaire a été préparé en concertation avec la Commission. Il précise l'économie de l'article L. 288 sur plusieurs plans bien distincts :

1° Il détermine les règles de procédure qui seront applicables dans le cas où la Commission — puis éventuellement les juridictions compétentes de l'ordre judiciaire — seraient amenées à mettre en œuvre la procédure de l'article L. 288 en cas de menace « d'atteinte grave et immédiate » à des droits et libertés, en enjoignant — ou ordonnant — aux administrations fiscales de prendre « sans délai » des mesures de sécurité particulières.

Ont été examinées à cette occasion la question de l'aménagement de la règle de quorum particulier applicable aux délibérations de la Commission concernant la mise en œuvre de l'article L. 288, les modalités de la transmission de l'injonction et du contrôle par la CNIL de la mise en œuvre de cette injonction, les règles applicables aux procédures suivies en première instance, en appel et en cassation, ainsi que la portée des décisions juridictionnelles rendues sur le fondement de l'article L. 288.

Le décret publié au journal officiel du 7 janvier 2000 (décret n° 2000-8 du 4 janvier 2000) ne reprend que de manière partielle les remarques émises sur ce point par la Commission dans sa délibération n° 99-047 du 14 octobre 1999, qui visaient à prendre pleinement en compte la spécificité de l'article L. 288, texte intervenant dans un domaine bien circonscrit et destiné à faire face, dans l'urgence, à des menaces graves et immédiates à des droits et libertés.

2° Sont également fixés les principes directeurs des dispositifs de sécurité des traitements automatisés comportant le NIR, d'une part, en précisant la nature des mesures à prévoir dans les demandes d'avis (celles-ci doivent concerner les sites où sont conservées les données, les traitements eux-mêmes, les agents bénéficiant d'une autorisation d'accès aux NIR, les conditions d'utilisation du NIR pour l'exercice du droit de communication, les dispositifs d'effacement des NIR et de destruction des supports), et d'autre part en posant le principe de l'intervention du haut fonctionnaire de défense pour surveiller l'exécution de ces mesures, « sans préjudice des pouvoirs conférés à la CNIL ».

3° Le texte comporte une liste indicative des mesures susceptibles d'être ordonnées par injonction « pouvant aller jusqu'à la destruction des supports d'information constitués à partir du NIR », qui est destinée à éclairer tant la CNIL que les administrations fiscales sur la portée de l'article L. 288.

4° Le texte limite les conditions dans lesquelles les agents de l'administration fiscale pourront utiliser le NIR dans le cadre de l'exercice du droit de communication, finalité qui avait été introduite dans le décret du 14 décembre 1999 après la consultation de la CNIL : il retreint la portée de cette seconde utilisation du NIR en la définissant par référence à la nécessité de confirmer l'identification d'une personne. Il encadre de manière stricte la conservation de cet identifiant dans les services locaux des impôts. Il limite, enfin, le nombre d'agents habilités par service à obtenir le NIR.

Délibération n° 99-033 du 24 juin 1999 portant avis sur un premier projet de décret en Conseil d'État pris pour l'application de l'article 107 de la loi du 30 décembre 1998

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 le code général des impôts et le livre des procédures fiscales ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ensemble le décret n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII de la loi précitée ;

Vu l'article 107 de la loi n° 98-1266 du 30 décembre 1998 portant loi de finances pour 1999, ensemble la décision n° 98-405 DC du 29 décembre 1998 du Conseil Constitutionnel ;

Vu le décret n° 85-855 du 7 août 1985 relatif à l'utilisation par la direction générale des impôts du répertoire national d'identification des personnes physiques ;

Vu l'arrêté du 7 août 1985 relatif à la création d'un traitement automatisé pour la simplification des procédures d'imposition, modifié par arrêtés des 28 avril 1987, 5 janvier 1990, 21 février 1994 et 9 août 1995 ;

Vu la lettre de saisine du Ministre de l'Économie, des finances et de l'industrie et du Secrétaire d'État au Budget en date du 15 juin 1999, ensemble une « note au ministre », une fiche technique et un projet de décret en Conseil d'État « pris pour l'application de l'article 107 de la loi n° 98-1266 du 30 décembre 1998 et complétant la deuxième partie du livre des procédures fiscales » précédé du « rapport au Premier Ministre » ;

Après avoir entendu Monsieur Noël CHAHID-NOURAÏ en son rapport, Monsieur Christian SAUTTER, Secrétaire d'État au Budget, en ses observations, ainsi que Madame Charlotte-Marie PITRAT, Commissaire du Gouvernement, également en ses observations ;

Considérant que le Ministre de l'Économie, des finances et de l'industrie et le Secrétaire d'État au Budget ont saisi la Commission nationale de l'informatique et des libertés (CNIL) d'un projet de décret en Conseil d'État « pris pour l'application de l'article 107 de la loi n° 98-1266 du 30 décembre 1998 et complétant la deuxième partie du livre des procédures fiscales », en éclairant ce projet par le « rapport au Premier Ministre » qui précise le contexte et la portée du projet, une lettre exprimant les intentions des ministres compétents et leurs engagements, une « note au ministre », ainsi qu'une « fiche sur le dispositif technique d'intégration du NIR dans les fichiers des administrations financières » ;

Considérant que c'est compte tenu de ce cadre général dans lequel le projet de décret s'insère qu'il y a lieu pour la Commission d'examiner le texte qui lui est soumis ; qu'il importe toutefois, au préalable, de rappeler les conditions et limites dans lesquelles le pouvoir réglementaire exerce sa compétence ;

Sur les conditions et limites de la mise en œuvre de l'article 107 de la loi de finances pour 1999

Considérant que l'article 107 de la loi de finances susvisée autorise la direction générale des impôts (DGI), la direction générale de la comptabilité publique (DGCP) et la direction générale des douanes et droits indirects (DGDDI) :

— à collecter, conserver et échanger entre elles les numéros d'inscription au répertoire national d'identification des personnes physiques (NIR) pour les utiliser exclusivement dans les traitements des données relatives à l'assiette, au contrôle et au recouvrement de tous impôts, droits, taxes, redevances ou amendes et aux seules fins d'accomplissement de ces missions (article L. 287 nouveau du livre des procédures fiscales — LPF),

— à utiliser ce numéro pour les demandes, échanges et traitements nécessaires à la communication, aux organismes chargés de la gestion d'un régime obligatoire de sécurité sociale et aux institutions de retraite complémentaire, des informations nominatives nécessaires à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions ainsi qu'à leur recouvrement (article L. 152 modifié du LPF) ;

Considérant, en outre, que le même article 107 de la loi de finances susvisée prévoit que, lorsqu'est exercé le droit de communication prévu à l'article L. 81 du LPF, les informations nominatives communiquées, sur tout type de support, par les personnes ou organismes autorisés à utiliser le NIR à l'égard desquelles ce droit peut légalement s'exercer, mentionnent le NIR (article L. 81 A nouveau du LPF) ;

Considérant, enfin, que l'article 107 de la loi de finances susvisée étend l'obligation de secret professionnel aux informations dont il s'agit et prévoit, dans le cas où la mise en œuvre du droit de communication s'avérerait susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi susvisée du 6 janvier 1978 dite « Informatique et libertés », la faculté pour la CNIL d'enjoindre l'autorité administrative de prendre sans délai les mesures de sécurité pouvant aller jusqu'à la « destruction des supports d'informations qui ont été constitués à partir d'un NIR » (article L. 288 nouveau du LPF) ;

Considérant que les précisions ainsi apportées par le législateur en ce qui concerne les finalités et les modalités de l'utilisation du NIR par les administrations financières ainsi que les garanties énoncées par lui au cas particulier correspondent à une volonté reposant elle-même sur la conviction, depuis longtemps ancrée en France, qu'il importe de demeurer particulièrement attentif aux risques qu'induit pour les libertés l'utilisation extensive et sans limites ni sauvegardes d'un identifiant national, généraliste et au surplus particulièrement signifiant, conviction qui se trouve d'ailleurs à l'origine même de la législation nationale sur l'informatique et les libertés ; qu'en effet, tout d'abord, ainsi que le rappelait déjà le rapport du Conseiller d'État TRICOT dès 1975, « plus l'identifiant sera commun à de nombreux services de l'État, des autres collectivités publiques et des grandes entreprises, plus il y aura à la fois de commodité à interconnecter et de désir de le faire » alors que de telles interconnexions, en permettant l'appariement de multiples données concernant les mêmes personnes sans leur aval, peuvent conduire à une connaissance approfondie de leur situation individuelle ; qu'en outre, en l'absence de finalités précisément assignées et strictement cantonnées, une logique d'extension se trouve engagée ; que par ailleurs, les caractéristiques de l'identifiant NIR, particulièrement signifiant à la différence de la plupart des identifiants étrangers, induisent le risque de sélections immédiates de catégories entières de population sur la base de certains des champs composant le numéro, notamment ceux qui correspondent à la naissance à l'étranger et au département ou pays de naissance ; qu'en toute hypothèse, son utilisation non contrôlée risque d'entraîner des traitements non personnalisés des situations individuelles, voire l'engagement d'actions selon des critères discriminants et par suite non légitimes ; que l'évolution récente de l'informatique et les progrès techniques qu'elle enregistre ne permettent pas

de nuancer sensiblement l'ensemble de ces appréciations ; qu'enfin, notre histoire nationale, même la plus récente, offre des illustrations concrètes de troubles imprévus et de dérives individuelles ;

Considérant que, de même, lors de l'examen par le Conseil Constitutionnel de sa constitutionnalité, c'est en raison des risques inhérents à un tel dispositif que la disposition en cause n'a été admise qu'au prix de réserves d'interprétation concernant d'une part la limitation stricte de sa portée et d'autre part les précautions qu'appelle sa mise en œuvre ;

Considérant, en premier lieu, qu'il résulte de la décision du Conseil Constitutionnel que la portée de l'article 107 est restreinte à des finalités définies de manière précise et limitative ; qu'en effet, selon le Conseil, la loi « se borne » à permettre aux administrations financières concernées d'utiliser le NIR « en vue d'éviter les erreurs d'identité et de vérifier les adresses des personnes », dans le cadre de leurs missions respectives, ainsi qu'à l'occasion des transferts autorisés de données, soit au bénéfice des administrations concernées dans le cas de l'exercice du droit de communication, soit au bénéfice des organismes de protection sociale visés à l'article L. 152 du LPF ; qu'en outre, s'agissant de la mention du NIR à l'occasion des communications au profit des organismes de protection sociale, « ces communications doivent être strictement nécessaires et exclusivement destinées à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions, ainsi qu'à leur recouvrement » ;

Considérant, en second lieu, que, selon le Conseil, la constitutionnalité du dispositif est établie sous réserve, également, de quatre garanties dont est assortie la mise en œuvre de l'article 107 de la loi de finances susvisée, savoir le respect du secret professionnel, la pleine application des dispositions protectrices de la liberté individuelle et de la vie privée établies par la législation relative à l'informatique, aux fichiers et aux libertés, l'interdiction d'utiliser le NIR pour la constitution de fichiers nominatifs sans rapport direct avec les opérations incombant aux administrations financières et sociales ou pour la mise en œuvre de tout nouveau transfert d'informations nominatives entre administrations et, enfin, l'existence d'une faculté d'intervenir conférée à la CNIL « lorsque la mise en œuvre du droit de communication prévu aux articles L. 81 A et L. 152 s'avère susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi nº 78-17 du 6 janvier 1978 » ;

Considérant que le projet de décret en Conseil d'État soumis à l'examen de la Commission, qui complète la partie réglementaire du livre des procédures fiscales, précise les conditions et les objectifs de la collecte du NIR par les administrations financières et les modalités des communications d'informations fiscales aux organismes chargés de la gestion d'un régime obligatoire de sécurité sociale et aux institutions de retraite complémentaire prévues à l'article L. 152 du LPF ; que s'il ne comporte pas de dispositions relatives à la conservation du NIR ni de mesures de sécurité, le projet de décret prévoit que l'application de ses dispositions n'interviendrait qu'à compter de l'entrée en vigueur d'un décret pris à cet effet ; que les dispositions du projet sont éclairées par l'ensemble des indications fournies par les ministres concernés ; que c'est à la lumière de ces engagements et décisions que doit être apprécié le projet soumis à la Commission ;

En ce qui concerne les finalités

Considérant que les auteurs de la saisine ont clairement manifesté leur volonté de donner toute sa portée à la décision du Conseil Constitutionnel en ce qui concerne les réserves relatives aux finalités de l'utilisation du NIR ; qu'en effet, d'une part, le « rapport au Premier Ministre » assigne au NIR comme objectif d'éviter les erreurs d'imposition et que le projet d'article R* 287-2 nouveau du LPF doit être rédigé en sorte que le NIR soit exclusivement collecté aux fins de gestion de l'identifiant fiscal spécifique — le numéro SPI ; que d'autre part, les administrations financières prévoient de limiter la fonction du NIR à celle d'un outil administratif de contrôle par exception, dont la vocation serait cantonnée à la vérification et à la certification de l'identité et de l'adresse des personnes et dont l'utilisation serait limitée à cette seule finalité ; que, notamment, le NIR ne serait pas utilisé pour la communication avec les contribuables, cette fonction étant assurée par le numéro SPI qui serait inscrit à compter de l'année 2001 sur les documents fiscaux adressés aux personnes physiques ayant la qualité de contribuable ; qu'en outre, l'utilisation du NIR devrait être entourée de toutes les précautions nécessaires afin que le recours à cet identifiant conserve un caractère exceptionnel, après épuisement de toutes les autres modalités d'identification du contribuable ; qu'enfin, toutes garanties ont été données en ce qui concerne la mise en œuvre de l'interdiction d'utiliser le NIR dans les échanges avec les banques ;

Considérant que les projets d'arrêtés concernant les traitements fiscaux appelés à comporter le NIR devant être examinés par la Commission à la lumière des observations qui précèdent et des dispositifs informatiques précisément spécifiés qui accompagneront les projets, il n'y a pas lieu à ce stade de regarder ce projet de décret lui-même comme devant être modifié à cet égard ;

En ce qui concerne les garanties

Considérant, en premier lieu, que si l'exploitation du NIR dans des services déconcentrés de la DGI et de la DGCP n'est pas de nature à entraîner, directement et par elle-même, la méconnaissance de l'obligation de secret, il importe, en tout état de cause, qu'afin d'assurer la sécurité des locaux de traitement du NIR l'adoption de mesures adéquates soit garantie, telles que l'administration des traitements par des agents spécialement habilités, la sécurisation physique et logique des sites de gestion et d'exploitation du NIR, ainsi que la mise en place des moyens nécessaires interdisant tout accès non autorisé aux fichiers comportant le NIR et de procédures de journalisation des requêtes, destinées à assurer le respect de cette mesure ;

Considérant, en deuxième lieu, qu'aucune disposition du projet de décret ne prévoit de nouvelle extension de la sphère d'utilisation du NIR ; qu'en outre, la restriction du nombre des fichiers contenant le NIR limite le risque de dissémination involontaire ; qu'enfin, des assurances ont été données qu'aucune nouvelle demande de dissémination ne serait formée, notamment au bénéfice des banques et compagnies d'assurance ; que ces garanties et engagements sont suffisants ;

Considérant, en troisième lieu, que l'article L. 288 nouveau du LPF ne saurait être regardé comme sans portée dès lors que le législateur l'a introduit dans le texte applicable pour donner une garantie supplémentaire et que le Conseil Constitutionnel en a fait une mention particulière ; que, par ailleurs,

cette disposition ne saurait être regardée comme redondante avec les dispositions du 3° de l'article 21 de la loi du 6 janvier 1978 dès lors que son champ d'application est plus large que celui des « circonstances exceptionnelles », seules visées à cet article, et que ses modalités de mise en œuvre sont plus précises ; qu'ainsi cette disposition, inspirée directement de préoccupations anciennement exprimées par la CNIL, vise une gamme d'hypothèses de gravité inégale et de nature différente dans lesquelles les dangers de l'interconnexion seraient sérieux ; que sa mise en œuvre incombera à la CNIL qui portera les appréciations nécessaires et formulera les prescriptions qu'elle jugera appropriées, sous le contrôle du juge le cas échéant ; que pour pouvoir remplir son plein effet, cette disposition implique, d'une part, que ses modalités d'application soient précisées comme il sera dit ci-après, d'autre part que, dans le cas où la mesure ordonnée par la CNIL serait la « destruction des supports qui ont été constitués à partir d'un NIR », elle puisse recevoir application et qu'à cette fin, il puisse être garanti que la destruction sera complète, immédiate et contrôlable par la CNIL ;

Considérant que la DGCP et la DGDDI prévoyant exclusivement l'intégration du NIR dans des fichiers nationaux, l'exécution des mesures prescrites en cas de mise en œuvre de l'injonction de destruction prévue à l'article L. 288 ne devrait pas présenter de difficultés en ce qui les concerne ; que, s'agissant de la DGI, le projet soumis à la CNIL, qui prévoit de limiter le traitement du NIR dans les fichiers tenus dans 16 centres régionaux d'informatique (CRI) suscite encore des interrogations au regard des critères rappelés ci-dessus et exige donc que des dispositifs adéquats et performants soient mis en œuvre ; que la réduction à 6 du nombre des CRI en 2003 annoncée par les ministres sera de nature à faciliter l'exécution des mesures et contrôles nécessaires ;

Considérant en outre que la Commission, lorsqu'elle sera saisie d'un second projet de décret prévoyant les mesures de sécurité nécessaires à l'application de l'article L. 288 du LPF, sera à même d'apprécier si les mesures envisagées sont de nature à répondre aux exigences de l'article L. 288 du LPF ;

Considérant, en quatrième lieu, qu'ainsi qu'il a été rappelé ci-dessus, le Conseil Constitutionnel a énoncé que « le législateur n'a pu entendre déroger aux dispositions protectrices de la liberté individuelle et de la vie privée établies par la législation relative à l'informatique, aux fichiers et aux libertés » ;

Considérant que si, au nombre des règles ainsi visées, figure l'obligation de soumettre à la CNIL les arrêtés régissant les traitements automatisés d'informations nominatives, les auteurs de la saisine se sont engagés à soumettre à cet égard les modifications des traitements existant dans lesquels le NIR se trouverait introduit ; qu'à l'occasion de l'examen de ces arrêtés, la CNIL se prononcera au cas par cas sur leur conformité à la législation « Informatique et libertés » et à l'article 107 de la loi de finances pour 1999 ainsi qu'à ses décrets d'application, en s'inspirant à cette occasion des précédents développements ;

Considérant qu'aux termes de l'article 5 de la Convention du 28 janvier 1981 du Conseil de l'Europe, « les données à caractère personnel faisant l'objet d'un traitement automatisé sont : (...) b) enregistrées pour des finalités déterminées (...) c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » ; que, selon le Conseil Constitutionnel, le législateur a « déterminé » de manière précise et limita-

tive les finalités de l'utilisation du NIR par les administrations financières ; que le NIR doit, en outre, être regardé comme adéquat, pertinent et non excessif pour autant qu'il ne se trouve pas mis en œuvre dans des conditions non strictement proportionnées à ces finalités ;

Considérant à cet égard qu'ainsi qu'il a été dit ci-dessus, les finalités envisagées dans le projet de décret n'excèdent pas celles qui ont été identifiées par le Conseil Constitutionnel, cette appréciation étant opérée sous réserve des observations qui précèdent et de celles qui pourraient être formulées lors de l'examen des projets d'arrêtés concernant les traitements destinés à comporter le NIR ; qu'ainsi le principe de proportionnalité doit être regardé comme étant respecté à ce stade ;

Sur certaines dispositions particulières du projet de décret soumis à la Commission

En ce qui concerne la collecte du NIR par les administrations financières (futur article R 287-1 du LPF)*

Considérant qu'il est prévu par le projet de décret soumis à l'examen de la Commission que le NIR serait collecté notamment auprès de l'Institut national de la statistique et des études économiques et, de manière exceptionnelle, auprès des personnes physiques tenues de souscrire une déclaration d'impôt sur le revenu, en application des articles 170 et 170 bis du code général des impôts, ou redevables, à quelque titre que ce soit, de tout impôt, droit, taxe, redevance, pénalité ou amende, savoir dans les seules hypothèses suivantes :
— à l'occasion du paiement de la taxe d'habitation et des taxes foncières établies au titre de l'année 2000,
— à l'occasion de la première souscription d'une déclaration d'impôt sur le revenu,
— dans le cadre de demandes de renseignement spécifique, lorsque la connaissance du NIR est nécessaire à la vérification et à la certification de l'identité du contribuable ;

Considérant que la collecte du NIR auprès des contribuables aurait, surtout après la généralisation du numéro SPI, un caractère exceptionnel, et serait motivée par le souci d'empêcher que des décisions ne soient prises par erreur à l'encontre d'un homonyme du contribuable concerné ; que la réponse du contribuable conserverait un caractère purement facultatif, les personnes concernées se voyant offrir l'option de communiquer ou non leur NIR ; qu'en outre le caractère facultatif de la demande du NIR devrait également résulter de ce qu'il serait demandé, en toute hypothèse, au contribuable de s'identifier auprès de l'administration fiscale en communiquant par priorité le numéro SPI si celui-ci lui a déjà été transmis ; que les auteurs de la saisine prévoient que les documents comportant le NIR transmis par les contribuables seront, d'une part, distincts des formulaires habituellement utilisés par l'administration fiscale, et d'autre part, transmis directement à un service central particulier, chargé des opérations de fiabilisation du NIR ;

Considérant que si le législateur n'a pas explicitement prévu une telle collecte auprès des personnes physiques, une telle collecte peut être admise dès lors, d'une part, qu'elle a pour seule finalité l'une de celles qui ont été reconnues par le Conseil Constitutionnel et qu'elle interviendrait à titre exceptionnel, d'autre part, sous réserve que soit assurée la mise en œuvre efficace des

garanties prévues ; que les modalités susmentionnées paraissent en l'état satisfaisantes au regard de telles garanties sous réserve de l'examen ultérieur des arrêtés relatifs aux fichiers qui seraient appelés à comporter le NIR ;

Considérant, par ailleurs, que le projet de décret pourrait utilement prévoir la mention systématique, sur les documents produits à l'intention des contribuables, de l'identifiant fiscal spécifique SPI ;

En ce qui concerne la conservation du NIR par les administrations financières

Considérant que le projet de décret soumis à la Commission, ainsi que le prévoit son article 4, serait complété par un second texte réglementaire, pris après avis de la CNIL, qui arrêterait les mesures relatives à la conservation du NIR par les administrations concernées en vue d'assurer la mise en œuvre des garanties dont le Conseil Constitutionnel a estimé qu'elles constituent une des conditions de la constitutionnalité de la loi ;

Considérant que ce nouveau projet de décret en Conseil d'État devrait préciser la nature des dispositifs de sécurité que les administrations financières s'engagent à mettre en œuvre ainsi que les procédés de contrôle et de mise en œuvre des mesures envisagées dans le cas de l'application des dispositions de l'article L. 288 ;

Considérant enfin que l'article 107 de la loi de finances pour 1999, en autorisant les administrations financières à faire usage du NIR pour certaines finalités et sous réserve du respect de garanties, rend désormais sans objet l'ensemble des dispositions du décret du 7 août 1985 relatif à l'utilisation du répertoire national d'identification des personnes physiques pour la gestion du traitement automatisé dénommé SPI ; que, d'ores et déjà, l'article 3 du projet de décret pourrait donc se trouver modifié en procédant à l'abrogation pure et simple du texte réglementaire précité ;

En ce qui concerne l'utilisation du NIR à l'occasion des transferts d'informations

Considérant que l'identité d'une personne ne pouvant se réduire à un numéro matricule, des échanges et communications d'informations appelés à comporter le NIR ne doivent pouvoir être mis en œuvre que si ce numéro est accompagné des éléments d'état civil des personnes concernées ; que, d'ailleurs, les risques très réels d'erreur induits par l'utilisation exclusive de chiffres peuvent être lourds de conséquence pour les contribuables comme pour les administrations financières, dont la responsabilité pourrait alors se trouver engagée ; que dès lors, les rapprochements d'informations susceptibles d'être effectués par ces administrations à partir de données communiquées par des tiers doivent tenir compte de l'ensemble des éléments d'identification transmis afin de s'assurer de l'identité des personnes concernées et de garantir la fiabilité des informations produites ; qu'en effet, s'il peut être admis que le NIR comporte des éléments de l'identité d'une personne, il ne saurait s'y substituer ;

Considérant, en outre, que dans le cas où les documents provenant de tiers déclarants et rattachés à un dossier fiscal sur la base d'un traitement automatisé feraient apparaître des divergences sur l'état civil ou l'adresse de la personne alors même que les numéros identifiants utilisés seraient concordants,

des vérifications complémentaires devraient être mises en œuvre avant toute utilisation des informations ;

Considérant en tout état de cause que le Conseil Constitutionnel ayant subordonné la constitutionnalité de la disposition législative au respect des finalités identifiées par lui et ayant rappelé, à cet effet, que les informations communiquées à la DGI au titre de l'article L. 152 modifié du LPF étaient exclusivement destinées à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions et à leur recouvrement, le projet de décret devrait faire interdiction de faire usage, à d'autres fins, des informations communiquées à la DGI à cette occasion ;

Considérant, par ailleurs, que la liste des organismes destinataires et le détail des informations communiquées par la DGI dans chaque cas seront fixés dans le cadre des arrêtés interministériels prévus par le décret pour préciser les modalités d'application de chacun des traitements ;

Considérant qu'afin d'éviter la conservation par un organisme de protection sociale d'informations financières dont il n'aurait pas dû normalement avoir à connaître par suite d'une erreur dans la constitution du fichier des demandes d'informations en violation des dispositions de l'article L. 152 ou par suite d'un changement dans la situation personnelle de la personne concernée au regard de la législation sociale, les allocataires, assurés sociaux et pensionnés devraient être tenus informés de la liste des organismes destinataires, sur le fondement de l'article L. 152, d'informations nominatives les concernant ; que cette communication serait de nature à les mettre en mesure d'exercer, s'il y a lieu, le droit de rectification ouvert par l'article 36 de la loi du 6 janvier 1978 en cas d'absence de prise en compte de l'évolution de leur situation personnelle au regard de la législation sociale ; que, dès lors, le projet de décret pourrait être complété en ce sens ;

Estime que le projet de décret d'application de l'article 107 de la loi de finances soumis à la Commission par les ministres compétents peut, au bénéfice de l'ensemble des observations présentées ci-dessus, recevoir un **avis favorable**.

Délibération n° 99-047 du 14 octobre 1999 portant avis sur un projet de décret en Conseil d'État relatif aux mesures de sécurité prévues par l'article L. 288 du livre des procédures fiscales

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le code général des impôts et le livre des procédures fiscales, notamment ses articles L. 81, L. 81 A, L. 152 et L. 288 ;

Vu le nouveau code de procédure civile ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ensemble le décret nº 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII de la loi précitée ;

Vu l'article 107 de la loi n° 98-1266 du 30 décembre 1998 portant loi de finances pour 1999, ensemble la décision n° 98-405 DC du 29 décembre 1998 du Conseil Constitutionnel ;

Vu le décret n° 80-243 du 3 avril 1980 relatif aux attributions des hauts fonctionnaires de défense ;

Vu la délibération de la CNIL n° 99-033 du 24 juin 1999 portant avis sur un premier projet de décret en Conseil d'État pris pour l'application de l'article 107 de la loi de finances pour 1999, ensemble, dans sa rédaction arrêtée au 30 septembre 1999 après avis du Conseil d'État, un « projet de décret pris pour l'application de l'article 107 de la loi de finances pour 1999 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects » ;

Vu la lettre de saisine du Ministre de l'Économie, des finances et de l'industrie et du Secrétaire d'État au Budget en date du 5 octobre 1999, ensemble un projet de décret en Conseil d'État « relatif aux mesures de sécurité prévues par l'article L. 288 du livre des procédures fiscales », précédé d'un « rapport au Premier Ministre » ;

Après avoir entendu Monsieur Noël CHAHID-NOURAÏ en son rapport et Madame Charlotte-Marie PITRAT, Commissaire du Gouvernement, en ses observations ;

Considérant qu'aux termes de l'article L. 288 ajouté au LPF par l'article 107 de la loi de finances susvisée : « Lorsque la mise en œuvre du droit de communication prévu aux articles L. 81 A et L. 152 s'avère susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la commission nationale de l'informatique et des libertés [CNIL] enjoint l'autorité administrative de prendre sans délai les mesures de sécurité pouvant aller jusqu'à la destruction des supports d'information qui ont été constitués à partir d'un numéro d'inscription au répertoire national d'identification des personnes physiques [NIR]. »

« Sans préjudice des dispositions de l'article 40 du code de procédure pénale, si cette injonction n'est pas suivie d'effet, la [CNIL] saisit le président du tribunal de grande instance de Paris, qui peut ordonner le cas échéant sous astreintes les mesures proposées par la Commission » ;

Considérant que le Conseil constitutionnel a, dans sa décision du 29 décembre 1998, estimé que la garantie constituée par ce dispositif donnant à la CNIL « la faculté d'intervenir » dans le cas susprécisé, figure au nombre des réserves auxquelles est subordonnée la conformité à la Constitution de l'ensemble de l'article 107 de la loi de finances pour 1999 ;

Considérant que la circonstance que la loi de finances pour 1999 n'ait pas envisagé que, pour son application, l'article L. 288 fasse l'objet d'un décret en Conseil d'État ne peut faire obstacle à l'exercice du pouvoir réglementaire en la matière ; qu'à la vérité, le dispositif de l'article L. 288, nécessite, pour être pleinement efficace dans certaines des circonstances qu'il vise, que soient aménagées les modalités procédurales de droit commun concernant l'intervention de la CNIL et l'action devant le juge judiciaire ; qu'en outre, l'article L. 288 du LPF sera rendu d'application plus aisée si se trou-

vent précisées les mesures de sécurité à appliquer par l'administration afin d'être en mesure de répondre le cas échéant aux injonctions de la CNIL ;

Considérant que c'est pour tenir compte de ce qui précède que les ministres ont pris l'engagement, lors de l'examen par la CNIL du projet de décret pris pour l'application de l'article 107 et relatif à l'utilisation du NIR par la direction générale des impôts (DGI), la direction générale de la comptabilité publique (DGCP) et la direction générale des douanes et droits indirects (DGDDI), qu'un autre décret en Conseil d'État préciserait « avant la fin de l'année les conditions et les modalités de déclenchement par la CNIL du processus de destruction du NIR » ; que cet engagement a été transcrit dans l'article 4 du projet de décret d'application de l'article 107 de la loi de finances susvisé qui prévoit, dans sa rédaction communiquée à la Commission, une disposition qui reporte l'application du texte à « l'entrée en vigueur du décret en Conseil d'État, pris après avis de la [CNIL] pour l'application de l'article L. 288 du LPF » ;

Considérant que c'est dans ce contexte que le Ministre de l'Économie, des finances et de l'industrie et le Secrétaire d'État au Budget ont saisi la CNIL d'un projet de décret en Conseil d'État « relatif aux mesures de sécurité prévues par l'article L. 288 du livre des procédures fiscales », précédé d'un « rapport au Premier Ministre », lequel en précise le contenu et la portée ;

Sur le titre et l'économie générale du projet

Considérant, en premier lieu, que le texte soumis à la CNIL comporte des dispositions de pure procédure et donc d'une autre nature que celles relatives aux mesures de sécurité, lesquelles au surplus trouvent normalement leur place dans les dossiers des arrêtés réglementaires régissant le fonctionnement des traitements ; qu'en outre, l'article 4 du projet de décret pris pour l'application de l'article 107 se réfère — ainsi qu'il a été rappelé ci-dessus — à un projet de décret « pris pour l'application de l'article L. 288 du livre des procédures fiscales » ; qu'ainsi le titre actuel du projet — « Décret relatif aux mesures de sécurité prévues par l'article L. 288 du livre des procédures fiscales » — ne correspond ni à son contenu, ni à l'article 4 du projet de décret pris pour l'application de l'article 107 ; que, par suite, pour des motifs de cohérence, de clarté et de précision, le titre du décret devrait indiquer qu'il se trouve « pris pour l'application de l'article L. 288 du livre des procédures fiscales » ;

Considérant, en second lieu, que l'économie générale du projet conduisant à distinguer deux catégories de dispositions — celles concernant la procédure et celles concernant les mesures de sécurité — l'articulation même du texte gagnerait à reprendre cette distinction en comportant deux sections, l'une regroupant les dispositions portant sur la procédure de mise en œuvre de l'article L. 288, l'autre consacrée aux mesures de sécurité prises pour l'application du même article ;

Considérant que le Gouvernement ayant exprimé son accord sur ces deux points, il y a lieu pour la Commission de prendre acte de cet accord ;

Sur les dispositions relatives à la procédure

Considérant que les dispositions relatives à la procédure doivent être établies en tenant compte d'une part de la nécessité, prévue par le législateur de 1998, d'une intervention « sans délai » destinée à faire face à une me-

nace « d'atteinte grave et immédiate » à des droits et libertés, d'autre part de l'importance que le Conseil Constitutionnel a accordé au dispositif de l'article L. 288 en soulignant, ainsi qu'il a été rappelé ci-dessus, que l'article 107 de la loi de finances susvisé n'était pas contraire à la Constitution « sous réserve des garanties dont est assortie sa mise en œuvre », l'article L. 288 constituant l'une de ces garanties ; qu'il y a lieu, dès lors, de prévoir un dispositif permettant une procédure pleinement efficace notamment en période de circonstances exceptionnelles, lesquelles ont été spécialement évoquées au cours des débats parlementaires ayant précédé le vote de la loi ;

En ce qui concerne l'aménagement de la règle relative au quorum applicable à la CNIL (article 3. I du projet)

Considérant que le projet de décret prévoit que la Commission peut valablement prendre les délibérations concernant « le pouvoir d'injonction » qui lui est attribué par l'article L. 288 du LPF « si cinq de ses membres en exercice sont présents, dont son président et l'un de ses vice-présidents » ;

Considérant que l'objet de cette disposition est d'assouplir la règle du quorum de neuf membres actuellement applicable afin de tenir compte des contraintes imposées par l'urgence et, le cas échéant, de conditions d'exception, et de garantir ainsi l'efficacité du dispositif quelles que soient les circonstances, sans pour autant que les responsabilités du bureau de la CNIL se trouvent méconnues ;

Considérant, toutefois, et en premier lieu, que ces exigences valant pour l'ensemble des délibérations concernant la mise en œuvre de l'article L. 288 et non pas seulement pour « le pouvoir d'injonction », il n'y a pas lieu de restreindre le champ de la disposition aux seules délibérations concernant l'exercice de ce pouvoir ;

Considérant, en second lieu, que l'objectif poursuivi par cette disposition serait atteint dans de meilleures conditions, eu égard à la circonstance qu'elle peut trouver à s'appliquer en période d'exception, si l'hypothèse de l'empêchement du président était expressément prévue ; qu'à cet effet il devrait être prescrit, aux fins de maintien d'une présence suffisante des membres du bureau et en conformité avec le droit commun — le remplacement du président par un vice-président étant de droit —, que dans un tel cas, la Commission peut valablement délibérer si cinq de ses membres en exercice sont présents, dont ses deux vice-présidents ;

En ce qui concerne les conditions de notification de l'injonction adressée à l'autorité administrative (article 3. III. 1re phrase)

Considérant que le projet soumis à l'examen de la Commission prévoit que la CNIL « fait parvenir son injonction par lettre recommandée avec demande d'avis de réception ou remise contre récépissé » ;

Considérant que cette disposition répondant à la nécessité de préciser les conditions de notification de l'injonction de la CNIL à « l'autorité administrative » en prévoyant des modalités adaptées, il importe, dans le même esprit, d'énoncer des précisions complémentaires sur le destinataire de la notification et les modalités d'acheminement aux services visés par elle ; qu'en conséquence, le décret devrait prévoir, d'une part que l'injonction prononcée par la CNIL en application de l'article L. 288 est notifiée au directeur général concerné, copie étant adressée au ministre chargé du budget, et

d'autre part que ce directeur général transmet sans délai l'injonction aux services visés par elle, s'il décide d'y déférer ;

Considérant que le Gouvernement ayant exprimé son accord sur ces points, il y a lieu pour la Commission de prendre acte de cet accord ;

En ce qui concerne les conditions de vérification de la mise en œuvre de l'injonction (article 3. III. 2e phrase)

Considérant que le projet transmis à la Commission prévoit, s'agissant de l'injonction, que celle-ci « peut désigner un ou plusieurs de ses membres pour assister à sa mise en œuvre » ;

Considérant que cette disposition correspond à la nécessité pour la CNIL, qui se trouve dotée par le législateur d'un pouvoir de saisine du juge dans le cas où l'injonction n'est pas suivie d'effet, d'être en mesure de déterminer par elle-même s'il y a lieu ou non de faire usage de cette faculté ; que, toutefois, la Commission ayant des pouvoirs de vérification aux termes du 2° de l'article 21 de la loi du 6 janvier 1978 susvisée — laquelle demeure applicable —, il importe que le ou les membres désignés par la Commission pour assister à la mise en œuvre des mesures prescrites puissent également être mandatés pour « vérifier sur place » si l'injonction a été suivie d'effet et qu'ils puissent se faire accompagner à cette fin « d'agents » de la Commission et « d'experts » ainsi que la loi du 6 janvier 1978 le prévoit ;

Considérant que le Gouvernement ayant exprimé son accord sur ces points, il y a lieu pour la Commission de prendre acte de cet accord ;

En ce qui concerne la procédure devant le président du tribunal de grande instance (article 3. IV)

Considérant que le projet de décret soumis à la CNIL prévoit que « Lorsque la Commission nationale de l'informatique et des libertés saisit le président du tribunal de grande instance de Paris en application du deuxième alinéa de l'article L. 288 du [LPF], elle présente sa demande dans les formes prévues pour les référés » et que « La décision rendue en la forme des référés est exécutoire à titre provisoire sauf si le président en décide autrement » ;

Considérant que, s'agissant de parer à une menace « d'atteinte grave et immédiate » à des « droits et libertés » par un recours au juge judiciaire, lequel ordonnera « sous astreintes » des mesures qui, normalement, auraient du être appliquées « sans délai », la procédure devant ce juge doit être marquée par le souci d'éviter tout retard ; qu'un tel résultat pourrait être mieux atteint si, outre la prévision actuellement envisagée, le texte du décret prévoyait expressément pour l'assignation le recours à la procédure du référé d'heure à heure du second alinéa de l'article 485 du nouveau code de procédure civile (NCPC), si le texte fixait au juge pour statuer un délai de 24 heures, de caractère non comminatoire, et si la décision juridictionnelle bénéficiait de l'exécution provisoire de plein droit, sous réserve de l'application de l'article 524 du NCPC ;

En ce qui concerne les voies de recours (article 3. IV. dernier alinéa)

Considérant que le projet de décret soumis à la CNIL prévoit que : « Le délai d'appel est de trois jours. Le président de la chambre saisie fixe à bref délai l'audience à laquelle l'affaire sera appelée. Au jour indiqué, il est procédé

selon les modalités prévues aux articles 760 à 762 du nouveau code de procédure civile » ;

Considérant que les exigences sus-rappelées relatives à l'urgence devraient conduire à faire application en la circonstance, non de la procédure d'appel de droit commun telle qu'organisée par les articles 760 à 762 du NCPC mais de la procédure à jour fixe prévue aux articles 788 à 792 du NCPC ; qu'en outre, et pour le même motif, il y aurait lieu de fixer le délai du pourvoi en cassation à trois jours courant à compter du prononcé de la décision attaquée et de conditionner l'inscription au rôle du pourvoi à la justification par le demandeur de l'exécution de la décision frappée de pourvoi, sauf décision contraire du Premier Président prise après avis du procureur général et des parties ;

Considérant, sur le dernier point, que la disposition suggérée, qui est d'ailleurs appelée à constituer prochainement le droit commun, a pour seul effet de désigner le demandeur pour lui faire supporter le cas échéant la charge de prouver l'absence de nécessité d'exécution afin d'être exonéré de son obligation d'exécuter et ne réduit nullement le pouvoir d'appréciation du Premier Président ; qu'elle ne saurait en aucune manière être regardée comme impliquant par elle-même la destruction des fichiers fiscaux comportant le NIR et ne saurait donc être écartée pour ce motif ;

Sur les dispositions concernant les mesures de sécurité

Considérant qu'il résulte des dispositions combinées des articles 15, 19 et 20 de la loi du 6 janvier 1978 susvisée que les dispositifs de sécurité des traitements automatisés trouvent normalement leur place dans les dossiers de demande d'avis sur les arrêtés réglementaires pris après avis motivé de la CNIL auquel il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État ; que toutefois il peut être admis, compte tenu du caractère global de la réforme qui concerne trois directions générales et de la spécificité de certaines mesures à prendre pour mieux garantir l'application dans des conditions satisfaisantes de l'article L. 288 du LPF, que soient fixés dans un décret quelques principes directeurs dont s'inspireront les arrêtés réglementaires susmentionnés ;

Considérant, dès lors, que peuvent être incluses dans le projet de décret à la fois des mesures de sécurité de caractère permanent et des mesures que la CNIL peut notamment enjoindre à l'autorité administrative de prendre sans délai en cas de menace grave et immédiate pour les droits et libertés ;

En ce qui concerne les mesures de sécurité de caractère permanent concernant les traitements (article 1er) et destinées à assurer la mise en œuvre effective de l'article L. 288 (article 4)

Considérant que le projet soumis à la Commission prévoit en son article 1er, dans sa rédaction actuelle, que « Les sites où sont implantés les fichiers comportant le [NIR] détenus par [la DGI, la DGCP et la DGDDI] font l'objet de mesures de sécurité déterminées dans les arrêtés régissant le fonctionnement des traitements automatisés sous le contrôle du haut fonctionnaire de défense relevant du ministre chargé de l'économie et des finances selon les modalités prévues par le décret du 3 avril 1980 » et que « Les agents qui administrent ces fichiers et en gèrent les traitements reçoivent une autorisation d'accès délivrée par le directeur général des impôts, le directeur géné-

ral de la comptabilité publique ou le directeur général des douanes et droits indirects » ;

Considérant, en outre, que l'article 4 du projet de décret est ainsi rédigé : « Pour chaque fichier [comportant le NIR] et leurs sauvegardes, il est institué un dispositif informatique centralisé permettant un effacement des [NIR], immédiat, complet et contrôlable par la [CNIL]. »

« En cas de défaillance de ce dispositif centralisé, un dispositif installé dans les centres informatiques permet l'effacement de ces numéros dans chaque lieu d'implantation d'un ou de plusieurs fichiers les contenant. Les agents qui mettent en œuvre ce dispositif sont désignés par le directeur général des impôts, le directeur général de la comptabilité publique ou le directeur général des douanes et droits indirects et habilités par le haut fonctionnaire de défense relevant du ministre chargé de l'économie et des finances. »

« Les noms et les fonctions des agents habilités à mettre en œuvre [ces dispositifs] sont communiqués à la [CNIL]. »

« Un compte-rendu d'exécution de ces procédures d'effacement est transmis à la [CNIL]. » ;

S'agissant des mesures prévues à l'article 1er

Considérant, en premier lieu, qu'il peut être utile au sein du ministère chargé du budget de confier à un seul haut fonctionnaire le soin de surveiller dans un souci de cohérence et d'homogénéité l'exécution des mesures de sécurité concernant trois directions générales ; qu'il peut en outre sembler judicieux que ce haut fonctionnaire soit doté d'une expérience du type de celle acquise par le haut fonctionnaire de défense visé par le décret du 3 avril 1980 précité, lequel confère notamment à l'intéressé la responsabilité de l'application des dispositions relatives à la sécurité des systèmes d'information et lui donne, à cette fin, autorité sur l'ensemble des directions et services placés sous l'autorité du ministre qu'il a pour mission d'assister ; que, toutefois, la compétence dévolue au haut fonctionnaire de défense par la disposition pertinente du projet relative aux mesures de sécurité ne saurait faire obstacle à ce que le niveau général et le détail desdites mesures soient déterminés dans les arrêtés régissant le fonctionnement des traitements, pris en application des articles 15, 19 et 20 de la loi du 6 janvier 1978, ni à ce que s'exerce pleinement le contrôle, tant préalable qu'a posteriori, de la CNIL sur ces mêmes mesures ;

Considérant, en second lieu, que les mesures prévues à l'article 1er doivent concerner non seulement la sécurité physique des sites où sont mis en œuvre les traitements comportant le NIR et où sont conservées les informations correspondantes ainsi que les agents chargés des opérations de gestion, mais aussi la sécurité logique des traitements eux-mêmes ;

Considérant que le Gouvernement ayant exprimé son accord de principe pour une clarification du projet de décret sur ces différents points, il y a lieu pour la Commission de prendre acte de cet accord ;

S'agissant des mesures prévues à l'article 4

Considérant qu'il peut être utile de prévoir des dispositions spéciales en vue de garantir l'application effective, le cas échéant et le jour venu, de mesures d'exception susceptibles d'être décidées par la CNIL dans ses injonctions ;

que toutefois s'il est envisagé de consacrer un article du décret à l'organisation d'un dispositif technique cohérent en vue de garantir l'effacement, en tant que de besoin, des NIR détenus par les administrations fiscales, une telle disposition doit nécessairement comporter également un dispositif correspondant à la mesure de destruction des supports d'information constitués à partir d'un NIR, cette mesure étant expressément envisagée par le législateur et l'effacement du NIR n'en tenant pas lieu ;

Considérant que, dans ces conditions, le décret devrait prévoir qu'en vue de permettre une mise en œuvre immédiate, complète et contrôlable par la CNIL, des mesures décidées par celle-ci, les arrêtés régissant le fonctionnement des traitements automatisés précisent les dispositifs et procédures permettant non seulement l'effacement des NIR mais aussi la destruction des supports d'information constitués à partir d'un tel numéro ;

Considérant que le Gouvernement ayant exprimé son accord de principe sur ce point, il y a lieu pour la Commission de prendre acte de cet accord ;

En ce qui concerne les mesures de sécurité à prendre pour l'exercice du droit de communication (article 2)

Considérant que, dans sa rédaction initiale soumis à l'examen de la Commission et au vu de laquelle a été adoptée la délibération du 24 juin 1999 susvisée, le premier projet de décret d'application de l'article 107 de la loi de finances pour 1999 prévoyait que le NIR est exclusivement collecté par les administrations fiscales « aux fins de gestion de l'identifiant fiscal national (numéro SPI) » ; que la lettre se saisine de la CNIL du 15 juin 1999 précisait que le NIR ne serait « présent [...] que dans les bases nationales situées dans des lieux uniques [...] ainsi que, s'agissant de la DGI, dans les seize centres régionaux de l'informatique (qui seront ramenés à six avant la fin 2003) » et que « De 1300 pour la DGI, les lieux d'utilisation du NIR seront donc réduits à 16, puis à 9 » ; que la Commission a, par sa délibération précitée, pris acte de la volonté exprimée par le Gouvernement de « limiter la fonction du NIR à celle d'un outil administratif de contrôle par exception, dont la vocation serait cantonnée à la vérification et à la certification de l'identité et de l'adresse des personnes et dont l'utilisation serait limitée à cette seule finalité [et d'entourer l'utilisation du NIR] de toutes les précautions nécessaires afin que le recours à cet identifiant conserve un caractère exceptionnel, après épuisement de toutes les autres modalités d'identification du contribuable » ; que la délibération a noté également que le texte « doit être rédigé en sorte que le NIR soit exclusivement collecté aux fins de gestion de l'identifiant fiscal spécifique SPI » ;

Considérant qu'il ressort toutefois de l'examen du projet de premier décret transmis à la CNIL à l'occasion de l'examen du présent texte que, dans le dernier état de sa rédaction, ce texte implique désormais que toutes les unités locales d'assiette et de recouvrement pourront utiliser le NIR dans l'exercice du droit de communication ; que, la question de la sécurité dans les centres locaux se trouvant désormais posée de manière spécifique en raison de cette modification du projet initial du Gouvernement, celui-ci envisage dans le second projet de décret que « les agents autorisés à consulter le [NIR] pour l'exercice du droit de communication mentionné aux articles L. 81 et suivants du [LPF] reçoivent une habilitation délivrée par le directeur général des impôts ou le directeur général de la comptabilité publique » ;

Considérant, à la vérité, que l'utilisation dont il s'agit, qui ne saurait constituer une nouvelle finalité du NIR, devrait être limitée à la confirmation — dans le cadre du droit de communication et par une personne habilitée à disposer du NIR — de l'identité et de l'adresse de certains contribuables, après épuisement de tous autres moyens d'identification ; qu'un tel recours au NIR à l'occasion de l'exercice du droit de communication se traduisant nécessairement par son utilisation dans les nombreux centres locaux en charge de l'assiette ou du recouvrement des impôts, toutes mesures doivent être prises pour empêcher la dissémination et la conservation du NIR, sur quelque support que ce soit, à l'intérieur des unités locales d'assiette et de recouvrement une fois l'opération de confirmation réalisée ; qu'à défaut en effet, le cantonnement de ce numéro aux seules fins d'identification se trouverait compromis, les mesures de sécurité prévues en cas d'atteinte grave et immédiate aux droits et libertés se trouveraient privées d'efficacité et le contrôle immédiat et complet de la CNIL sur leur mise en œuvre deviendrait impossible ;

Considérant qu'en conséquence il importe, en premier lieu, dans chaque unité locale, de limiter à deux le nombre des agents qui reçoivent une habilitation personnelle, délivrée par le directeur général dont il relèvent et les autorisant à consulter le NIR conservé dans les traitements fiscaux aux seules fins de confirmation de l'identité de la personne physique concernée par l'exercice du droit de communication, en deuxième lieu, de mettre en œuvre des mesures de sécurité adéquates dans tout centre où se trouve exercé le droit de communication afin d'interdire l'accès non autorisé aux traitements comportant le NIR, en troisième lieu, de garantir que le centre ne pourra conserver trace du numéro sur quelque support que ce soit et quelle qu'en soit l'origine une fois obtenue la confirmation de l'identité du contribuable faisant l'objet de la demande ; que ces mesures devraient être déterminées dans les arrêtés régissant le fonctionnement des traitements automatisés ;

Considérant que le Gouvernement ayant donné son accord pour que le projet de décret soit complété dans le sens de ce qui vient d'être dit, il y a lieu pour la Commission de prendre acte de cet accord ;

En ce qui concerne la liste indicative des mesures susceptibles d'être ordonnées par injonction (article 3. II)

Considérant qu'afin d'éclairer la CNIL et les services sur le type de mesures susceptibles d'être décidées par injonction par la Commission, il peut être utile de faire figurer dans le texte du projet de décret une liste non exhaustive et purement indicative de ces mesures ; qu'à cette fin, le projet de décret fournit une telle liste ainsi constituée :
— renforcement de la sécurité physique des centres informatiques de la DGI, de la DGCP ou de la DGDDI affectés au traitement des NIR ;
— retrait à titre provisoire ou définitif de l'autorisation d'accès à un agent ou à un groupe d'agents en charge de la gestion des traitements comportant le NIR,
— retrait à titre provisoire ou définitif de l'habilitation personnelle autorisant d'obtenir des services chargés de la gestion du NIR le numéro d'une personne physique pour l'exercice du droit de communication,
— suspension provisoire de l'utilisation du NIR par la DGI, la DGCP ou la DGDDI dans les missions prévues aux articles L. 81 A et L. 152 du livre précité,
— effacement définitif d'un ou plusieurs NIR contenus dans un ou plusieurs des fichiers mentionnés à l'article 8, dans leurs sauvegardes ainsi que,

comme l'accepte le Gouvernement, dans les copies de fichiers réalisées à des fins techniques ;

Considérant que cette liste devrait être complétée en ce qui concerne le renforcement des mesures de sécurité physique et logique pour le traitement et la conservation des informations dans les services informatiques habilités à gérer le NIR, le renforcement des conditions de l'accès à distance aux informations et de leur transmission en application des articles L. 81 A et L. 152 du LPF, ainsi que la destruction, dans un ou plusieurs sites de mise en œuvre des traitements, d'un ou plusieurs supports d'information constitués à partir d'un NIR — notamment la réduction du nombre des sauvegardes et des copies de travail —, cette dernière mesure ayant pour objet d'envisager une étape supplémentaire, adaptée à l'hypothèse d'une crise grave mais localisée, avant la destruction de tous les supports d'information comportant ou permettant de reconstituer le NIR ;

Considérant que le Gouvernement ayant donné son accord pour que le texte soumis à la CNIL soit complété en ce sens, il y a lieu pour la Commission de prendre acte de cet accord ;

Est d'avis que le projet de décret pris pour l'application de l'article L. 288 du livre des procédures fiscales devrait être modifié selon les orientations sus-précisées.

D. L'application du nouveau dispositif dans les traitements de l'administration fiscale

A la suite de ces deux délibérations, la Commission a été saisie par le ministère de l'économie, des finances et de l'industrie de deux demandes d'avis modificatives visant à autoriser la direction générale des impôts à enregistrer le NIR dans :
— la base de données nationale dénommée « SPI » (« Simplification des Procédures d'Imposition »),
— les chaînes de traitements « SIR » (« Simplification de la gestion des informations de recoupement ») qui sont préalables à la centralisation des données dans les fichiers nationaux permanents « SIR ».

Les modifications apportées au fichier national des contribuables « SPI » sont conformes aux garanties exigées par la CNIL dans les avis précédents. Il s'agit à titre principal de mettre en place la « table de correspondance NIR/n° SPI », d'assurer l'échange d'informations entre la DGI et l'INSEE aux fins de certification des informations d'identité concernant les personnes connues de la DGI et de transmission des NIR correspondants, et de déterminer les mesures de sécurité applicables à la « table de correspondance NIR/n° SPI », y compris le dispositif permettant un effacement du NIR et la destruction des supports d'information constitués à partir de ce numéro.

Lors de l'examen de ces demandes, la CNIL s'est assurée d'une part, que les projets qui lui étaient soumis répondaient bien aux principes posés par la Commission à l'occasion de l'examen des deux décrets d'application, qui tiennent aux finalités du NIR, aux conditions de son enregistrement et de son utilisation ainsi qu'au respect des garanties prévues par la loi et détaillé par les décrets, d'autre part, que leur contenu comportait la description précise de l'ensemble des dispositifs de

sécurité dont les principes directeurs ont été énumérés par le « second décret d'application ».

Il résulte du travail d'instruction accompli par la CNIL que le NIR sera exclusivement conservé, dans le cadre de l'application « SPI », dans une « table de correspondance NIR / n° SPI », le traitement « SPI » étant installé sur un ordinateur dédié. Une réplication de la « table de correspondance NIR/SIR » gérée par le traitement « SPI » sera également conservée ; elle sera indépendante, physiquement et logiquement, des fichiers « SIR ». Seuls deux centres informatiques disposeront des tables de correspondance. Les sauvegardes de la table de correspondance seront exclusivement entreposées, dans chacun des deux sites, dans un robot à cartouches situé dans la salle ordinateur, dont l'accès est contrôlé par un système de badge. Les seuls fichiers contenant des NIR qui proviendront d'autres CRI résulteront de la saisie de « déclarations papier » qui sont du même type que ceux fournis directement dans le cadre des procédures informatisées de transfert de données sociales (TDS).

S'agissant des modalités d'accès et d'intervention applicables aux tables de correspondance, seuls les agents d'exploitation des centres de calcul auront accès aux informations dans de strictes conditions contrôlées par la Commission.

Enfin, s'agissant des mesures de destruction des supports d'information constitués à partir du NIR, un dispositif informatique permettant de déclencher à distance un effacement de la table de correspondance sera mis en place, tant pour le fichier lui-même que pour ses sauvegardes. Le processus d'effacement des supports sera entièrement traçable. En cas de défaillance du dispositif centralisé, un dispositif au sein du CRI permettra l'effacement de la table. Un compte rendu d'exécution de ces procédures d'effacement sera transmis à la CNIL. La destruction s'effectuera, pour les sauvegardes, par incinération. Les disques comportant le NIR feront l'objet, à la demande de la CNIL, de mesures de destruction physique. Enfin, la sécurisation des transferts de données sur support informatique entre CRI ou avec des organismes tiers et la méthode d'évaluation de la sécurité des sites informatiques ont été définies en parfaite coopération avec le ministère.

Ainsi, les exigences de la loi du 6 janvier 1978 auxquelles a renvoyé l'article 107 de la loi de finances, à savoir l'examen par une autorité indépendante, de l'ensemble des mesures d'application d'une disposition législative, au demeurant contestée, ont-elles été de nature tout à la fois à cantonner et sécuriser l'usage du NIR par une nouvelle administration habilitée à l'utiliser et, surtout, à prévenir, voire empêcher toute nouvelle diffusion du NIR.

Il appartient désormais à l'administration concernée d'appliquer fidèlement les dispositifs prévus et à la CNIL d'exercer une surveillance vigilante sur cette application, compte tenu des risques inhérents à un numéro… pas comme les autres.

Délibération n° 99-060 du 9 décembre 1999 portant avis sur deux demandes d'avis modificatives prévoyant l'intégration du NIR dans les traitements « SPI » et « SIR »
(Modification des demandes d'avis nº 101969 et 104337)

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le code général des impôts et le livre des procédures fiscales ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ensemble le décret nº 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII de la loi précitée ;

Vu l'article 107 de la loi nº 98-1266 du 30 décembre 1998 portant loi de finances pour 1999, ensemble la décision nº 98-405 DC du 29 décembre 1998 du Conseil Constitutionnel ;

Vu la délibération de la CNIL nº 99-033 du 24 juin 1999 portant avis sur un premier projet de décret en Conseil d'État pris pour l'application de l'article 107 de la loi de finances pour 1999 ; ensemble, dans sa rédaction arrêtée au 30 septembre 1999 après avis du Conseil d'État, un « projet de décret pris pour l'application de l'article 107 de la loi de finances pour 1999 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects » ;

Vu la délibération de la CNIL nº 99-047 du 14 octobre 1999 portant avis sur un second projet de décret en Conseil d'État, relatif aux mesures de sécurité prévues par l'article L. 288 du livre des procédures fiscales ; ensemble, dans sa rédaction transmise au Conseil d'État pour avis un projet de « décret pris pour l'application de l'article L. 288 du livre des procédures fiscales » ;

Vu l'arrêté du 7 août 1985 relatif à la création d'un traitement informatisé pour la simplification des procédures d'imposition, modifié par les arrêtés du 28 avril 1987, du 5 janvier 1990, du 21 février 1994 et du 9 août 1995 ;

Vu l'arrêté du 28 avril 1987 relatif à la création d'un traitement informatisé de simplification de la gestion des informations de recoupement, modifié par les arrêtés du 31 janvier 1989, du 19 avril 1995, du 4 décembre 1996, du 18 février 1997, du 4 août 1997, du 21 janvier 1998 et du 14 avril 1998 ;

Vu les projets d'arrêtés modificatifs présentés par le ministère de l'Économie, des finances et de l'industrie ;

Après avoir entendu Monsieur Noël CHAHID-NOURAÏ 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 a été saisie par le ministère de l'Économie, des finances et de l'industrie de deux demandes d'avis modificatives visant à autoriser la direction générale des impôts (DGI) à enregistrer le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR), d'une part dans le fichier na-

tional des contribuables dénommé « SPI » (« Simplification des Procédures d'Imposition »), d'autre part dans le cadre de l'application « SIR » (« Simplification de la gestion des informations de recoupement ») dont la finalité principale est de faciliter l'exploitation par les services fiscaux des informations issues des déclarations fiscales annuelles à la charge des organismes versant à des tiers des revenus imposables, au moyen de leur rapprochement avec les résultats du traitement des déclarations de revenus et de la mise en œuvre de dispositifs automatisés d'aide aux opérations de contrôle sur pièces ;

Considérant que ces demandes d'avis et les deux projets d'arrêtés modificatifs qui les accompagnent, trouvent leur fondement dans l'article 107 de la loi de finances pour 1999, qui autorise notamment à collecter et conserver les NIR pour les utiliser exclusivement dans le traitement des données relatives à l'assiette, au contrôle et au recouvrement de tous impôts, droits, taxes, redevances ou amendes et aux seules fins de l'accomplissement de ces missions (article L. 287 nouveau du livre des procédures fiscales — LPF) ;

Considérant également que l'article 107 de la loi de finances susvisée étend l'obligation de secret professionnel aux informations dont il s'agit et prévoit, dans le cas où la mise en œuvre du droit de communication s'avérerait susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi susvisée du 6 janvier 1978 dite « Informatique et libertés », la faculté pour la CNIL d'enjoindre l'autorité administrative de prendre sans délai les mesures de sécurité pouvant aller jusqu'à la « destruction des supports d'informations qui ont été constitués à partir d'un NIR » (article L. 288 nouveau du LPF) ;

Considérant que le projet de « décret pris pour l'application de l'article 107 de la loi de finances pour 1999 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects » prévoit, dans sa rédaction arrêtée après avis du Conseil d'État, la création, dans le LPF, d'un article R. 287 ainsi rédigé :

« [Les NIR] sont utilisés exclusivement :
1) pour vérifier la fiabilité des éléments d'identification des personnes physiques figurant dans les traitements de données relatives à l'assiette, au contrôle et au recouvrement de tous impôts, droits, taxes redevances ou amendes,
2) pour l'exercice du droit de communication auprès des personnes énumérées à l'article R. 81 A. « ;

Considérant que l'article 4 du projet de « décret pris pour l'application de l'article L. 288 du livre des procédures fiscales », dans sa rédaction transmise au Conseil d'État pour avis, est ainsi rédigé :

« Les demandes d'avis sur les traitements automatisés qui utilisent les numéros d'inscription au répertoire national d'identification des personnes physiques et sont décidés sur le fondement des articles 15, 19 et 20 de la loi du 6 janvier 1978 susvisée prévoient des mesures de sécurité concernant :
— les sites de la direction générale des impôts, de la direction générale de la comptabilité publique et de la direction générale des douanes et droits indirects où sont conservées les données ou mises en œuvre les traitements automatisés ;

— les traitements eux-mêmes ;
— les agents en charge de la gestion de ces traitements, qui reçoivent une autorisation d'accès délivrée par le directeur général compétent.

Les demandes mentionnées à l'alinéa précédent précisent les dispositifs permettant un effacement des numéros d'inscription au répertoire national d'identification des personnes physiques ainsi que la destruction des supports d'information constitués à partir d'un tel numéro.

Ces dispositifs permettent une mise en œuvre immédiate, complète et contrôlable par la Commission nationale de l'informatique et des libertés. (...) » ;

Considérant que le contrôle exercé par la Commission sur les arrêtés relatifs à l'enregistrement et à l'utilisation du NIR dans certains traitements de la DGI — et sur les dossiers de demande d'avis correspondants — qui lui sont soumis doit notamment porter sur la conformité de ces projets aux dispositions des projets de décret d'application de l'article 107, en l'absence de publication de ces textes ;

Considérant que les modifications apportées au traitement « SPI » se limitent à :
— la mise en place d'un fichier dénommé « table de correspondance NIR / n° SPI » qui, par ailleurs, est transmis au site informatique chargé de la gestion du traitement « SIR »,
— la mise en place d'échanges d'informations entre la DGI et l'INSEE aux fins de certification des informations d'identité concernant les personnes physiques connues de la DGI et de transmission des NIR correspondants,
— la définition des mesures de sécurité applicables à la « table de correspondance NIR/n° SPI », y compris le dispositif permettant un effacement du NIR et la destruction des supports d'information constitués à partir de ce numéro,
— un aménagement des conditions d'exercice du droit de rectification pour les données transmises par l'INSEE ;

Considérant que les modifications apportées au traitement « SIR » prévoient :
— la fiabilisation des informations de recoupement provenant des déclarations des tiers-déclarants, par l'utilisation du NIR qui n'est pas enregistré dans l'application « SIR »,
— l'enregistrement du NIR dans les fichiers temporaires de déclarations annuelles, notamment ceux issus de la saisie, dans un nombre limité de centres régionaux d'informatique (CRI) de la DGI, des déclarations comportant le NIR qui sont effectuées sur support papier,
— l'utilisation, par le site informatique en charge de la gestion de « SIR », d'une copie de la « table de correspondance NIR/n° SPI » afin de procéder au remplacement, dans les fichiers permanents de « SIR », du NIR des fichiers temporaires par le n° SPI, seul identifiant utilisé dans « SIR » à l'occasion des traitements d'aide au contrôle fiscal et dans le cadre des échanges de données avec les autres applications de la DGI,
— l'impossibilité, pour les services utilisateurs du traitement « SIR », de consulter la « table de correspondance NIR/n° SPI » qui y est associée ;

Considérant qu'ainsi, le NIR sera exclusivement présent dans un fichier informatisé dénommé « table de correspondance NIR / n° SPI », créé en relation avec le traitement « SPI » à partir des réponses de l'INSEE aux demandes de

la DGI de certification de l'état civil des contribuables, et répliqué pour être également utilisé dans le cadre du traitement « SIR » ;

Considérant que ce fichier a pour fonction de mettre en parallèle, pour chaque personne physique présente dans le fichier « SPI », le NIR qui lui est affecté par l'INSEE et l'identifiant national fiscal qui lui est attribué par la DGI ; qu'il permettra de substituer le numéro SPI au NIR sur les déclarations annuelles de revenus imposables transmises à l'administration fiscale par les tiers déclarants qui en disposent ;

Considérant que les mesures de sécurité dont seront entourés la mise en œuvre de ce fichier et les transferts de fichiers informatisés comportant le NIR entre CRI ou avec des organismes tiers feront l'objet de mesures de sécurité, actées dans les demandes d'avis et différents documents complémentaires adressés ultérieurement à la CNIL et rappelées dans l'annexe jointe qui fait partie intégrante de la présente délibération ;

Considérant qu'un nouvel article doit être ajouté dans les arrêtés modificatifs relatifs aux traitements « SPI » et « SIR », afin de fixer le principe de la gestion du NIR dans un fichier distinct ; que cet article devrait être rédigé comme suit :

« Les numéros d'inscription au répertoire national d'identification des personnes physiques sont exclusivement conservés dans des fichiers informatisés dédiés, dénommés » table de correspondance NIR/n° SPI « , qui permettent d'établir un lien fixe entre le NIR et l'identifiant fiscal national individuel qui est normalement utilisé par les administrations fiscales dans leurs traitements internes et dans les relations avec les contribuables. Ces fichiers sont enregistrés sur des supports informatiques distincts et font l'objet de mesures de sécurité renforcées. » ;

Considérant, par ailleurs, que le projet d'arrêté relatif au traitement « SPI » prévoit que le droit de rectification s'effectue, pour ce qui concerne les informations certifiées sur la base du répertoire national d'identification des personnes physiques (RNIPP) de l'INSEE, non pas auprès du centre des impôts territorialement compétent mais de l'INSEE ;

Considérant cependant qu'une telle conception, si elle était adoptée par l'ensemble des organismes habilités à interroger l'INSEE pour faire certifier les éléments d'état civil en leur possession, reviendrait à confier à l'INSEE une nouvelle mission tendant à assurer la gestion commune et l'uniformisation des éléments d'identité des personnes physiques contenus dans les fichiers publics certifiés par ses soins ; qu'en outre, une telle conception ignorerait l'article 37 de la loi du 6 janvier 1978 qui dispose que « un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenu dans ce fichier. » ; qu'en conséquence, le paragraphe III de l'article 1er du projet d'arrêté relatif au traitement « SPI », qui modifiait sur ce seul point l'article 9 de l'arrêté du 7 août 1985, doit être supprimé ;

Considérant, enfin, en ce qui concerne le traitement « SIR », que le recours au NIR sera limités aux déclarations en provenance des employeurs, des organismes et services chargés de la gestion d'un régime obligatoire de sécurité sociale, des institutions de retraite complémentaire et des institutions gestionnaires du régime de l'assurance-chômage ; que le NIR ne sera présent que dans la « table de correspondance NIR/n° SPI » et dans les chaînes

de traitements mises en œuvre préalablement à la centralisation, dans les fichiers nationaux permanents « SIR », des informations de recoupement ;

Émet un **avis favorable** aux projets d'arrêtés soumis à son examen, compte tenu des engagements pris en matière de sécurité tels que rappelés dans l'annexe jointe au présent avis et qui en fait partie intégrante, sous les réserves suivantes :

— la création, au sein des arrêtés « SPI » et « SIR » d'un nouvel article, ainsi rédigé :

« Les numéros d'inscription au répertoire national d'identification des personnes physiques sont exclusivement conservés dans des fichiers informatisés dédiés, dénommés » table de correspondance NIR/n° SPI « qui permettent d'établir un lien fixe entre le NIR et l'identifiant fiscal national individuel qui est normalement utilisé par les administrations fiscales dans leurs traitements internes et dans les relations avec les contribuables. Ces fichiers sont enregistrés sur des supports informatiques distincts et font l'objet de mesures de sécurité renforcées. »,

— la suppression du paragraphe III de l'article 1er du projet d'arrêté relatif au traitement « SPI ».

Annexe relative aux mesures de sécurité mises en place par la Direction générale des impôts concernant le traitement du NIR dans les applications « SPI » et « SIR »

I. En ce qui concerne le confinement du NIR dans des tables de correspondance NIR/SPI :

1) Le NIR est exclusivement conservé, dans le cadre de l'application « SPI », dans une « table de correspondance NIR/n° SPI ». Le traitement « SPI » est installé sur un ordinateur dédié [demandes d'avis du 21/10, lettre du 29/10].

2) Une réplication de la « table de correspondance NIR/SIR » gérée par le traitement « SPI » est conservée dans le site informatique en charge du traitement « SIR ». Elle est indépendante, physiquement et logiquement, des fichiers « SIR » [demandes d'avis du 21/10].

3) Les tables de correspondance seront conservées sur des fichiers dédiés et, à la demande de la CNIL, sur des supports informatiques distincts afin d'en rendre possible la destruction physique [lettres des 29/10 et 22/11].

4) Seuls les deux CRI gestionnaires de « SPI » et de « SIR » stockeront les données de la « table de correspondance NIR/n° SPI ». Il n'y aura pas de troisième site susceptible de servir de site de secours, puisque le processus de réplication des tables de correspondance entre les deux sites garantit l'intégrité physique des données [lettres du 29/10 et du 22/11].

5) Les sauvegardes de la table de correspondance seront exclusivement entreposées, dans chacun des deux sites, dans un robot à cartouches situé dans la salle ordinateur, dont l'accès est contrôlé par un système de badge [demandes d'avis du 21/10, lettre du 29/10].

6) Les seuls fichiers contenant des NIR qui proviendront d'autres CRI résulteront de la saisie de « déclarations papier » qui sont du même type que ceux fournis directement dans le cadre des procédures informatisées de transfert de données sociales (TDS) [lettre du 22/11].

II. En ce qui concerne les modalités d'accès et d'intervention applicables aux tables de correspondance :

1) Seuls les agents d'exploitation des centres de calcul auront accès aux informations. Les développeurs, chargés de concevoir l'évolution des traitements, mettent au point leurs programmes à partir de données fictives [lettre du 22/11].

2) Le nombre des agents d'exploitation qui pourront avoir accès aux tables de correspondance est limité. Dans le site informatique gestionnaire de « SPI », le chef d'exploitation, 1 analyste et 2 programmeurs système d'exploitation ont tous les droits (SYSADMIN) ; 4 préparateurs de travaux et 4 agents de traitements ont un accès limité au projet dont ils sont responsables. Dans le site gestionnaire de « SIR », 4 programmeurs système d'exploitation, dont le chef d'exploitation, ont tous les droits ; 4 programmeurs ont un accès limité au projet dont ils sont responsables [lettre du 22/11].

3) Dans les cas exceptionnels d'analyse d'incidents par l'équipe de développement sur les sites d'exploitation, les travaux seront effectués sous le contrôle des agents habilités dans le CRI et par des personnes soumises par contrat aux obligations relatives au secret professionnel. Le recrutement d'une assistance externe à l'exploitation est exceptionnelle [lettre du 22/11].

4) Seule la société fournisseur des matériels et systèmes d'exploitation est susceptible d'intervenir sur les matériels et logiciels système. Ces opérations de maintenance ne peuvent s'effectuer que sur accord et en présence d'un chef d'exploitation et/ou d'un administrateur système [lettre du 29/10].

5) Un stock de cartouches sera affecté à la sauvegarde de la « table de correspondance NIR/n° SPI ». Une procédure de gestion de ce stock et de destruction des cartouches devenues inutilisables sera mise en place. La destruction sera effectuée par incinération par des personnels de sociétés spécialisées en présence d'agents d'exploitation de la DGI. En conséquence, les cartouches ayant conservé le NIR ne seront jamais réutilisées à d'autres fins [lettre du 22/11].

6) La liste des opérations effectuées sur la table NIR/n° SPI au moyen de programmes utilitaires comportant une fonction de déchargement ou d'édition papier d'extraits sera établie et vérifiée chaque jour. Les utilitaires qui auraient une fonction unique de déchargement sur PC seront verrouillés [lettre du 22/11].

7) Les fichiers audit de l'ordinateur enregistrent les traitements qui administrent et utilisent la table de correspondance et les fichiers temporaires comportant le NIR. Ils sont sauvegardés par procédures automatiques sous la responsabilité du chef d'exploitation et/ou de l'administrateur système et sur CD-ROM [demandes d'avis du 21/10, lettres des 29/10 et 22/11].

8) Tout retrait physique d'une cartouche hors de son logement dans le robot à cartouches provoque un scannage de l'ensemble de la bibliothèque dont il est gardé trace. Les retraits peuvent donc être contrôlés par l'administrateur du robot à cartouches [lettre du 29/10].

III. En ce qui concerne la gradation des mesures de destruction des supports d'information constitués à partir du NIR qui sont envisagées :

1) Un dispositif informatique permettant de déclencher à distance un effacement de la table de correspondance est mis en place, pour le fichier

lui-même et ses sauvegardes. Le processus d'effacement des supports sera entièrement traçable [demandes d'avis du 21/10, lettre du 22/11].

2) En cas de défaillance du dispositif centralisé, un dispositif au sein du CRI permet l'effacement de la table [demandes d'avis du 21/10].

3) Un compte rendu d'exécution de ces procédures d'effacement est transmis à la CNIL [demandes d'avis du 21/10].

4) Les programmes mettant en œuvre la procédure d'effacement seront conservés dans une version de référence. Des comparaisons avec la version en exploitation seront effectués régulièrement. Une version d'exercice, qui permettra de simuler le bon fonctionnement de la procédure, sera implantée [demandes d'avis du 21/10].

5) La destruction s'effectuera, pour les sauvegardes, par incinération [lettre du 07/12].

6) Afin de répondre à une demande de la CNIL, les disques comportant le NIR pourront faire l'objet de mesures de destruction physique. [lettre du 22/11].

IV. En ce qui concerne la sécurisation des transferts de données sur support informatique entre CRI ou avec des organismes tiers :

1) Les transferts par réseau entre les sites informatiques gestionnaires des traitements « SPI » et « SIR » s'appuient sur le protocole X25 utilisé par Transpac au travers du groupe fermé d'abonnés de la DGI. Le protocole de transfert utilisé, CFT, ajoute un niveau de sécurité, tant par le codage qu'il induit par la compression que par les mécanismes spécifiques mis en œuvre : contrôle des droits d'accès, mots de passe, gestion des numéros d'appelants, gestion des profils et des objets [lettre du 29/10].

2) En ce qui concerne les procédures bilatérales relatives aux déclarations de salaires et/ou d'honoraires, de pensions et rentes, d'indemnités journalières de maladie, les envois de fichiers sont sécurisés : les tiers déclarants doivent adresser les supports informatiques en recommandé dans un emballage qui les protège d'éventuelles détériorations ; le site informatique gestionnaire de « SIR » accuse réception de l'envoi à l'émetteur si le programme de contrôle informatique ne fait apparaître aucune anomalie ; dans le cas contraire, le fichier refusé, accompagné d'une liste des anomalies détectées, est retourné à l'envoyeur [lettre du 22/11].

3) En ce qui concerne la procédure de transfert de données sociales (TDS) — mise en place avec la sécurité sociale —, l'intégralité des transferts doit être effectuée, à compter de 2000, par réseau Transpac, selon le protocole X25 [lettre du 22/11].

4) En cas de recours aux nouvelles technologies de type internet, la DGI adoptera les procédés de chiffrement qui seront recommandés par la prochaine loi sur la société de l'information (des études ont déjà été engagées) [lettre du 07/12].

5) Dans les cas où la DGI continuerait à recourir à des réseaux classiques, une évaluation des moyens supplémentaires de sécurité à mettre en œuvre pourrait être engagée [lettre du 07/12].

V. Sur l'évaluation de la sécurité des sites informatiques :

1) Le centre informatique gestionnaire de « SPI » fait l'objet d'un classement en « point sensible 1 » au sens de l'instruction générale interministérielle n° 4600/SGDN. Une commission relevant de la responsabilité du secrétariat général de le défense nationale vérifie régulièrement la conformité à ce classement des mesures de sécurité physiques prises. Une demande de classement du site en charge du traitement « SIR », identique au classement du CRI en charge de « SPI », sera prochainement présentée par la direction générale des impôts [demandes d'avis du 21/10, lettre du 29/10].

2) La DGI prend l'engagement de lancer, dans l'année à venir, une démarche d'évaluation (sous la responsabilité du service central de sécurité des systèmes d'information), au regard des critères internationalement reconnus (la norme ISO 15408), de la sécurité informatique en place dans les deux centres informatiques précités, démarche qui débouchera sur une définition d'objectifs (en vue d'une éventuelle mise à niveau des dispositifs existants dans les meilleurs délais) [lettre du 07/12].

COMMERCE ÉLECTRONIQUE : LA CONFIANCE EN JEU

La protection des données personnelles et de la vie privée constitue un enjeu majeur de la société de l'information. Toutes les déclarations des pouvoirs publics ou des acteurs du commerce électronique l'évoquent comme un élément indispensable pour établir la confiance sur Internet [1].

A l'heure où la France s'interroge de façon persistante sur le meilleur mode de régulation de l'internet, les résultats, rendus publics en mai 2000, d'une enquête réalisée par « Ipsos — Médiangles » et « Emap » sont sans ambiguïté. Si, à la différence de leurs homologues américains, 62 % des internautes français estiment que le fonctionnement d'internet ne se caractérise pas, pour l'heure, par une utilisation abusive des informations personnelles — preuve s'il en est que vingt ans de culture « informatique et libertés » en France irriguent incontestablement le réseau —, 86 % d'entre eux se déclarent en faveur de l'intervention de l'Etat pour réglementer l'usage des données personnelles ou pour préciser les règles de bonne conduite que doivent respecter les acteurs en cette matière.

Les 60 experts réunis en convention à la demande du Conseil européen pour rédiger le projet de Charte des droits fondamentaux qui doit compléter le traité de l'Union européenne, prévoient d'ailleurs, à l'aube de ce nouveau millénaire marqué par le triomphe de la société de l'information, d'inclure au rang des droits garantis dans toute l'Union européenne celui de la protection des données personnelles.

1 Tel était le sens du premier G7 sur la société de l'information réuni les 24-25 février 1995 par la Commission européenne à la demande des partenaires, et qui concluait à l'engagement des gouvernements à assurer une protection effective de la protection des données personnelles. La présentation du programme du gouvernement sur la société de l'information le 18 février 1999, le discours du Premier ministre à Hourtin le 24 août 1999 ou les déclarations des entreprises multinationales réunies dans l'initiative « Global Business Dialogue » le 13 septembre 1999 à Paris en témoignent également.

Pour sa part, la CNIL, jugeant qu'il convenait de passer du discours sur la protection des données personnelles à la mise en œuvre effective des droits des internautes a pris deux nouvelles séries d'initiatives au plan national et européen.

La première a constitué, après la mise en œuvre depuis janvier 1998 d'un vaste programme pédagogique à destination de la jeune communauté française des professionnels de l'internet [1], à réaliser une évaluation « informatique et liberté » de 100 sites de commerce électronique.

Les résultats de cette étude sont très encourageants, mais plusieurs éléments doivent conduire à poursuivre les efforts avec les professionnels et à rechercher de nouveaux moyens d'action. Les initiatives tendant à une labellisation des sites de commerce électronique, en tant qu'instrument pragmatique pour assurer la confiance, constituent à cette égard une opportunité particulièrement adaptée.

La seconde initiative concerne l'adoption d'un rapport incluant une série de recommandations sur le publipostage électronique et le « spam ». Ce rapport, qui a donné lieu à de nombreuses consultations des professionnels, a été établi dans le prolongement des travaux dont la Commission a rendu compte les années précédentes.

Ce rapport, qui a été rendu public notamment sur le site de la CNIL, a été porté par la CNIL à la connaissance de ses homologues européens. Il a servi de base à un travail au sein du groupe dit « de l'article 29 » des autorités indépendantes des Etats membres de l'Union européenne, qui a adopté un avis rendu public le 3 février 2000 [2] reprenant les analyses et recommandations de la CNIL (cf. annexe 11).

Au titre de ses missions en matière de sécurité, la CNIL se félicite des efforts entrepris par les pouvoirs publics au cours de la seule année 1999 pour, d'une part, libéraliser par la voie réglementaire l'accès aux techniques de chiffrement dit « fort » (décrets du 17 mars 1999) dans l'attente de l'initiative annoncée de nature législative [3], et, d'autre part, consacrer la signature électronique grâce à l'adoption de la loi du 29 mars 2000, compatible, avec les exigences européennes fixées dans la directive 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. Cette directive, dont la complète transposition requiert encore l'adoption de mesures réglementaires précisant les exigences techniques, est destinée à assurer la reconnaissance mutuelle des signatures électroniques au sein de l'Union européenne.

Il reste que les solutions techniques destinées à assurer la sécurité sur internet qui sont actuellement disponibles, et mises en œuvre avec succès, comme le montre l'évaluation des 100 sites effectuée par la CNIL, n'assurent en général que la confidentialité du seul numéro de carte bancaire et non toujours la confidentialité de l'ensemble de la transaction.

1 Janvier 1998 — diffusion du guide pratique et pédagogique « Je monte mon site » —, juillet 1998 — adoption et diffusion en ligne d'un formulaire de déclaration adapté aux sites internet accompagné de recommandations pratiques et d'exemples de mentions d'information sur les droits des internautes —, janvier 1999 — dématérialisation de la procédure de déclaration —, diffusion en mars 1999 de la liste des organismes qui en effectuant cette déclaration se sont engagés à respecter les droits des internautes.

2 Cet avis est consultable sur le site de la Commission européenne : http://www.europa.eu.int/comm/dg15 à la rubrique protection des données, documents du groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dit « de l'article 29 »

3 CNIL-19e rapport d'activité 1998, page 85

Il reste également que les solutions pratiques pour l'identification sûre des partenaires d'une transaction électronique — commerciale ou non — méritent encore d'être approfondies qu'il s'agisse des techniques reposant sur la biométrie, en cours de développement, ou sur les puces électroniques dont l'usage est déjà bien éprouvé en France depuis les travaux de son inventeur français M. Roland Moreno.

Les « puces » en particulier, qui constituent une solution sûre puisque leur usage conduit à ce que ni leurs numéros ni les codes confidentiels qui leur sont attachés ne soient transmis sur le réseau, nécessitent cependant leur insertion sur un support et l'usage d'un lecteur.

Divers projets sont à l'étude ou en cours d'expérimentation. Les uns reposent sur la carte bancaire à puce, déjà à la disposition de la plupart des internautes pour le monde « hors ligne », qu'il convient de pouvoir insérer dans un lecteur connectable à l'ordinateur de l'internaute ou dans le téléphone portable permettant l'accès à internet. Mais les solutions disponibles sont encore coûteuses. Le prix actuel du lecteur de carte associé à l'ordinateur est d'environ 400 F, celui des téléphones portables à lecteur intégré de plus de 3000 F. D'autres solutions sont à l'étude reposant sur l'insertion directe dans les téléphones portables d'une puce spécifiquement destinée à l'identification en matière de transactions.

Enfin, de nouvelles préoccupations se font jour en relation avec le traitement de plus en plus sophistiqué des données de navigation de l'internaute sous forme de profils, le plus souvent non directement nominatifs, mais qui sont destinés à cibler les messages publicitaires en fonction de chaque profil individuel ou à personnaliser des services qu'un site ou un groupe de sites souhaitent offrir. Sur ce sujet, la Commission est également très sollicitée par plusieurs entreprises intervenant sur ces marchés qui estiment devoir répondre aux craintes des internautes en offrant des garanties de protection des données personnelles.

I. L'ÉVALUATION DE 100 SITES FRANÇAIS DE COMMERCE ÉLECTRONIQUE

A ce jour, plus de 4 000 organismes publics ou privés ont déclaré un ou plusieurs sites à la CNIL. La seule obligation déclarative des sites Internet n'est cependant pas suffisante pour assurer que le niveau de protection exigé par la loi du 6 janvier 1978 est systématiquement atteint. C'est pourquoi la Commission a procédé à une évaluation « informatique et libertés » de 100 sites de commerce électronique.

A. Méthodologie et présentation

Sur le plan méthodologique, le choix a été fait de ne retenir que des sites de commerce électronique au sens strict, c'est-à-dire des sites qui peuvent amener à accomplir un acte d'achat. Une liste de sites de commerce électronique a ainsi été arrêtée en tenant compte tout à la fois de l'importance du trafic généré par ces sites, tel

qu'il résulte de plusieurs études d'audience régulièrement diffusées sur Internet, de la notoriété de la marque ou de l'enseigne dans le monde réel ou sur Internet.

De fait, l'élaboration de cette liste a été guidée par le souci d'y faire figurer ceux des sites auxquels les internautes, d'aujourd'hui ou de demain, ont le plus de chance de se connecter. Cette liste, recouvrait les grands secteurs d'activité du commerce électronique : les produits culturels (livres, CD audio, CD Rom, billetterie...), informatique (matériels et logiciels), le tourisme (vols, hébergement), la vente de fleurs, la vente de vins, la grande distribution, l'automobile, l'alimentation, les sites réservés aux adultes, autres (vêtements, jouets...).

Enfin, cette liste devait comporter à la fois des « petits sites », des « sites autonomes » et des portails qui, par leur notoriété, constituent le passage d'entrée le plus fréquemment utilisé pour surfer sur le Web. Bien évidemment, d'autres secteurs d'activité pourraient ultérieurement faire l'objet d'une telle évaluation.

L'étude ne distinguait pas selon que les sites soumis à l'évaluation avaient ou n'avaient pas été déclarés à la CNIL.

B. Les enseignements

Au titre des bons résultats, les constatations suivantes ont été faites :
— 96 % des sites étudiés offrant la possibilité d'un paiement en ligne, sécurisent la transmission des coordonnées bancaires et 70 % donnent aux internautes une information complémentaire sur le procédé de sécurisation utilisé. Les sites manifestent le souci de recourir à des procédés de paiement sécurisés et de donner sur ce point des explications complémentaires aux internautes. Sur l'échantillon étudié, 90 sites sur 100 offrent la possibilité d'un paiement en ligne.
— 97 % des sites qui indiquent céder les informations collectées à des tiers partenaires commerciaux ou filiales, informent les internautes de leur droit de s'y opposer. Dans un cas sur deux, ce droit peut s'exercer en ligne grâce à une case à cocher. Ce résultat est bien supérieur à la pratique actuelle dans le monde réel où l'information se borne le plus souvent à signaler que les informations pourront être communiquées à des tiers (partenaires commerciaux) sans préciser — parce qu'en l'état la loi du 6 janvier 1978 ne l'impose pas explicitement — que chacun dispose du droit de s'opposer à une telle cession.
— 69 % des sites comportent une information spécifique sur la loi « informatique et libertés ». On observe que cette information est le plus souvent faite (dans plus de 40 % des cas) sur chacun des formulaires de collecte, c'est à dire à toute occasion où un internaute peut être amené à livrer des données personnelles. Dans 27 % des cas cette information est faite sur plusieurs formulaires de collecte mais pas sur tous, ce qui s'explique sans doute davantage par une négligence des responsables de sites que par une volonté délibérée.

Dans un nombre très substantiel de cas (plus de 30 %), une rubrique spécifique « informatique et libertés » est ouverte par le site, généralement accessible depuis la page d'accueil ou depuis le formulaire de collecte ou le bon de commande. Cette pratique qui est de nature à susciter la confiance mérite d'être encouragée.

S'agissant de la terminologie utilisée, il a été observé que dans 70 % des cas (soit 48 sites sur 69) c'est la « loi du 6 janvier 1978 » qui est évoquée, tandis que dans 22 % des cas (15 sites sur 69) il est fait référence à la « loi informatique et libertés ». La notion de « vie privée » n'apparaît que marginalement (3 %), la notion de « protection des données personnelles » davantage encore (1,5 %).C'est donc la référence à la loi (92 %) qui est première, ce dont il y a lieu de se féliciter. En outre, la forte notoriété de la loi du 6 janvier 1978 est confirmée. Enfin, le concept de protection des données personnelles ou à caractère personnel, qui est celui de la directive européenne est sans doute trop nouveau et trop abstrait pour évoquer quoi que soit à quiconque.

De nettes insuffisances ont également été observées.

Ainsi, 40 % des sites étudiés n'indiquent pas clairement l'adresse physique du responsable du site, alors que cette référence serait de nature à renforcer la confiance.

81 % des sites ne donnent aucune information sur l'usage qui peut être fait des cookies. Cela est regrettable compte tenu des craintes que cette technologie peut encore susciter et des usages le plus souvent légitimes que les sites concernés leur assignent (ex : relier entre eux pendant une session plusieurs achats en vue de l'établissement d'une facture récapitulative). Cette analyse est d'ailleurs confirmée par l'étude « Ipsos-Mégiangle » et « Emap » de mai 2000 qui indique que 92 % des internautes français réclament une explication sur la nature des informations communiquées automatiquement par leur ordinateur.

46 % des sites étudiés n'ont pas été déclarés à la CNIL. Cette situation est d'autant plus préjudiciable pour les consommateurs qu'une très forte corrélation est observée entre déclaration à la CNIL et qualité de l'information délivrée aux internautes.

Autre observation : le droit d'accès est le grand absent. 52 % des sites ne précisent pas le lieu où s'exerce le droit d'accès reconnu par nos législations. Ajoutons cependant que sur ces 52 sites qui ne le précisent pas, 3 d'entre eux mettent à disposition des internautes une *hot line* dédiée à la protection des données. Il demeure toutefois que la moitié des sites n'indiquent pas où s'exerce le droit d'accès. Ce résultat, qui peut paraître décevant, doit être cependant rapporté aux dispositions de la directive européenne du 24 octobre 1995 qui n'impose au responsable du traitement d'indiquer de manière systématique le lieu d'exercice du droit d'accès que lorsque cette information est nécessaire pour assurer à l'égard de la personne concernée un traitement loyal de ses données « (article 10 de la directive 95/46/CE).

Enfin, les sites « portails » et les plates — formes de commerce électronique ne paraissent pas actuellement jouer le rôle fédérateur qu'on pourrait attendre d'eux sur le plan de la protection des données. Le fait qu'un site de commerce soit affilié à un site portail ou à une plate-forme de commerce électronique ne paraît pas conduire à une meilleure qualité de l'information des internautes, alors même que les formulaires électroniques utilisés par les boutiques concernées sont le plus souvent normalisés.

Evidemment, les résultats de cette première étude n'ont pas valeur scientifique. Ils confirment cependant nettement l'attachement des sites français de commerce électronique à la protection des données personnelles. Mais, incontestablement la France peut mieux faire. La déclaration des sites à la CNIL — complètement dématérialisée — en constitue encore l'occasion. Elle est une manière de « labellisation publique », moment où la pédagogie et l'engagement déontologique se nouent.

Les résultats de cette étude ont par ailleurs été présentés à la conférence européenne des commissaires à la protection des données réunie les 6 et 7 avril 2000 à Stockholm, afin que l'Union européenne harmonise ses pratiques pour renforcer la confiance sur internet.

C. Les initiatives

La Commission a pris les initiatives suivantes en direction des différents acteurs.

1) LE RAPPEL À LA LOI

En direction des sites, la Commission a rappelé ceux qui n'avaient pas effectué la déclaration préalable à l'observation de la loi.

Ce rappel à la loi incluait également les précisions nécessaires à l'accomplissement des autres obligations des responsables de site prévues par la loi du 6 janvier 1978 en matière d'information des internautes : indiquer clairement l'identité et l'adresse physique du responsable du site, faire apparaître sur tout formulaire électronique de collecte d'informations le caractère obligatoire ou facultatif des réponses, au moyen par exemple d'un astérisque, et indiquer sur l'ensemble des formulaires si les données collectées seront ou non communiquées ou mises à la disposition de tiers non liés à la prestation, tels que des partenaires commerciaux, filiales, etc, et, dans l'affirmative, préciser aux personnes leur droit de s'y opposer. A cet égard, la Commission leur a fait part de sa recommandation que ce droit puisse s'exercer en ligne, par l'apposition, par exemple, d'une case à cocher. Le bien fondé de cette recommandation est d'ailleurs confirmé par l'opinion des 91 % d'internautes interrogés dans le cadre de l'étude d'« Ispos — Médiangle » de mai 2000 qui souhaitent pouvoir facilement informer le site de leur refus de voir leurs données utilisées.

Enfin, dans le souci de renforcer la confiance sur internet, la CNIL recommande aux sites de dédier une rubrique, accessible depuis la page d'accueil ou le formulaire de collecte, à la protection des données personnelles et à la vie privée, l'existence et le lieu d'exercice du droit d'accès pouvant utilement être précisé dans cette rubrique.

Par ailleurs, la CNIL estime que tous les sites auraient avantage à informer les internautes, compte tenu des craintes que les cookies peuvent encore susciter et

des usages le plus souvent légitimes que les sites concernés leur assignent, de leurs fonctionnalités et de leur éventuelle utilité.

2) LA MISSION DES ORGANISATIONS PROFESSIONNELLES

La Commission a invité les organisations professionnelles, les plates-formes et les portails de commerce électronique à jouer leur rôle de relais « informatique et libertés » auprès de l'ensemble des organismes ou des sites qu'ils fédèrent.

3) LA PROTECTION DES MINEURS

S'agissant de la protection des mineurs la Commission a engagé un travail de formulation de propositions d'information spécifique pour les sites susceptibles d'attirer les mineurs.

II. LA LABELLISATION DES SITES ET RELAIS « INFORMATIQUE ET LIBERTÉS »

La Commission a incité les organismes de labellisation des sites de commerce électronique qui sont appelés en pratique a jouer un rôle central dans la confiance que les internautes-consommateurs peuvent accorder aux commerçants qu'ils approchent, à intégrer la protection des données personnelles et de la vie privée dans leurs référentiels.

Ainsi, la Commission est-elle, d'ores et déjà en relation avec les deux organismes labellisateurs qui déclarent intervenir en France sur ce terrain dans le domaine du commerce électronique. Il s'agit d'une part, de L@beliste, lancé dans le cadre du Conseil national du commerce et de l'Institut international du commerce électronique, et crée par les deux fédérations des entreprises du Commerce et de la distribution (FED) et la FEVAD (Fédération des entreprises de vente à distance), d'autre part, de WebTrust, lancé par les experts comptables américains et canadiens, auquel les institutions professionnelles comptables françaises, la Compagnie nationale des commissaires aux comptes et l'Ordre des experts comptables ont décidé d'adhérer en vue de proposer un service de labellisation aux entreprises. Des initiatives de même nature sont en cours de préparation du côté des associations de consommateurs.

Cependant, les initiatives que recouvrent au plan national et international le vocable de « labellisation » et de « certification » des sites sont très diverses et à divers égards.

S'agissant des acteurs, il peut s'agir de sociétés spécialisées sur internet, de professionnels du contrôle, tels les auditeurs ou commissaires au compte, d'organisations professionnelles ou de protection des consommateurs, de banques, de portails, etc.

S'agissant de l'objet de la labellisation, il peut être très spécialisé ou, au contraire, étendu aux divers aspects de la confiance : l'authentification de l'identité du vendeur et du site, la sécurité des moyens de paiement et des transactions, l'information sur les produits et les conditions commerciales, la moralité d'un contenu éditorial, la protection des données personnelles, les procédures de règlement des litiges etc.

Les référents retenus sont également très divers. Il peut s'agir de règles de l'art (en matière technique par exemple), de recommandations déontologiques professionnelles, ou bien de règles posées par la loi ou la réglementation administrative.

S'agissant des méthodes et des procédures de délivrance et de retrait du label ou du certificat, les situations sont les plus diverses depuis la simple déclaration d'adhésion d'une entreprise sans qu'aucune vérification de la sincérité de cette adhésion ne soit opérée jusqu'à l'octroi du label par un organisme indépendant et après audit avec vérification régulière de la conformité au label.

Enfin, la portée et la couverture géographique du label peuvent être nationaux, régionaux ou mondiaux.

Dès lors, pour ne pas ajouter à la confusion des consommateurs, certaines clarifications devront être apportées et la question de la labellisation des labellisateurs en matière de protection des données se pose.

Pour la CNIL, cette question n'est pas d'une nature différente de celle traitée par la directive européenne à propos des codes de conduite qui distinguent les codes qui auront reçu un avis favorable des autorités de contrôle de protection des données des autres codes.

Dans ce contexte, la CNIL poursuit parallèlement deux séries d'actions :

— La première, « de terrain », est conduite au plan national et selon son approche pragmatique traditionnelle, avec les organismes français qui développent des procédures de labellisation. Dans ce cadre, le dialogue est lancé sur trois points. Tout d'abord s'agissant de l'objet des labels, la Commission s'attache à promouvoir la protection des données personnelles par référence aux principes posés par la loi et aux recommandations pratiques faites par la CNIL. La Commission étudie, par ailleurs, avec les professionnels les éléments clés de méthode et de procédure en vue d'assoir la crédibilité des labels de protection des données. Enfin, elle incite ces acteurs à partager les travaux engagés avec leurs homologues étrangers, européens ou des pays tiers impliqués.

— La seconde est conduite au plan européen pour promouvoir une approche commune de portée tout à la fois européenne et mondiale.

La CNIL a ainsi engagé ses homologues européens à mener une réflexion sur la création d'un label « EUP — European Union Privacy » articulée sur quatre éléments.

Tout d'abord, ce label pourrait être délivré par le groupe de l'article 29 ou par chacune des autorités nationales de contrôle des Etats-membres de l'Union européenne dès lors qu'un site s'engagerait : — à préciser la finalité du traitement des

données collectées (au moins lorsque cela s'impose, c'est-à-dire hors le cas où les données sont strictement nécessaires à la commande ou à la livraison),
— à préciser sur tout formulaire de collecte le caractère obligatoire ou facultatif des informations collectées,
— à préciser si les données collectées ne seront exploitées que par le site ou si elles seront cédées à des tiers, notamment à des fins de prospection commerciale,
— à mettre en mesure les internautes de s'opposer en ligne, par l'apposition d'une case à cocher sur tout formulaire de collecte, à la cession de leurs données à des tiers étrangers à la transaction (ce point constitue une garantie essentielle),
— à reconnaître un droit d'accès aux données collectées,
— à préciser les conditions de sécurité technique des transactions.

Ensuite, il pourrait être également envisagé de mettre en place au niveau européen un mécanisme de contrôle de qualité « EUP » des différents labels pouvant être délivrés par les organisations professionnelles européennes.

Dans ce contexte, le même label devrait pouvoir être délivré à une entreprise d'un pays tiers qui s'engagerait ainsi à respecter les exigences européennes de protection des données au profit notamment des internautes européens. De même la procédure envisagée pour le contrôle de qualité des labellisateurs devrait être ouverte aux organismes professionnels non européens délivrant un label de protection des données.

Enfin, la CNIL a proposé de soutenir avec vigueur toutes les initiatives professionnelles ou techniques (générateur de texte de l'OCDE dénommé « Wizard », le produit P3P développé par le consortium 3W) dès lors qu'elles satisferaient aux garanties minimales exigées par la directive européenne.

Le groupe de l'article 29 poursuit actuellement activement les travaux nécessaires à la réalisation de cette initiative.

III. LE RAPPORT ET LES RECOMMANDATIONS SUR LE PUBLIPOSTAGE ÉLECTRONIQUE ET LE « SPAM »

A. L'enjeu

Le « publipostage électronique » est l'envoi de messages électroniques à un ou plusieurs destinataires dont le nombre peut varier de quelques dizaines à plusieurs centaines de milliers, voire plusieurs millions. Il repose sur la collecte préalable d'adresses électroniques (e-mails) auxquelles seront adressés des messages électroniques.

Au regard des législations de protection des données personnelles, une adresse électronique est évidemment une information nominative : directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse ; en tout état

de cause, toujours indirectement nominative dans la mesure où toute adresse électronique est associée à un nom et à une adresse physique. De surcroît, à la différence d'autres catégories de données personnelles (numéro de téléphone, plaque minéralogique, etc.), une adresse électronique fournit dans bien des cas de nombreux renseignements sur la personne : son nom, son lieu de travail, son fournisseur de messagerie ou son fournisseur d'accès, son pays d'établissement, etc.

Le publipostage électronique peut être un support de communications de natures différentes : commerciale, bien évidemment, mais aussi politique, ou relevant du prosélytisme religieux, cultuel ou sectaire, ou encore concernant des produits ou services à caractère pornographique, etc.

Cette activité fait actuellement l'objet d'un important débat, en Europe, aux Etats-Unis et dans l'ensemble de l'internet, presque exclusivement consacré à la prospection commerciale électronique.

La forme la plus controversée de publipostage électronique est appelée « spamming ». Cette expression trouve son origine dans un sketch des Monty Python, dans lequel deux personnes parlant de saucisson, répètent le mot « spam » tous les deux ou trois mots (« spam »), jusqu'à (« spam ») l'exaspération (« spam ») des spectateurs (« spam ») !

Le « spamming » est l'envoi massif — et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc.

Les formes les plus contestées de « spamming » consistent pour l'expéditeur à falsifier ou à masquer son identité ou encore à usurper l'adresse électronique d'un tiers, afin de ne pas être identifié.

Le « spamming » a tendance à monopoliser le débat actuellement en cours sur les garanties qui devraient être reconnues aux personnes susceptibles de faire l'objet d'opérations de publipostage électronique. Il ne constitue, cependant, qu'une des formes de publipostage électronique.

Le rapport élaboré suite aux travaux engagés l'année dernière ainsi qu'à la demande du gouvernement dans le cadre des travaux relatifs à l'adoption d'une directive européenne sur certains aspects du commerce électronique [1] a été adopté le 14 octobre 1999. Il est disponible sur le site de la CNIL.

Au regard des règles de protection des données personnelles, le problème posé par le publipostage électronique est double :
— il s'agit, tout d'abord, de déterminer les conditions dans lesquelles des données personnelles (ici, l'e-mail) peuvent être collectées et utilisées à des fins de prospection ;

1 Le texte de cette directive adopté le 4 mai 2000 par le Parlement européen dans les mêmes termes que celui de la position commune du Conseil des ministres n'est pas encore paru au JOCE.

— il s'agit, ensuite, d'apprécier les garanties qui doivent être mises en œuvre pour permettre aux personnes, le cas échéant, de s'opposer à faire l'objet de prospections.

B. La méthode de travail

La méthode de travail a comporté, outre l'étude des garanties reconnues en Europe à l'égard de l'ensemble des autres modes de démarchage, la consultation des acteurs et l'étude des droits et pratiques hors de l'Union européenne.

Les organismes ou associations, à compétence nationale ou internationale, qui ont été consultés dans le cadre de cette étude étaient représentatifs des acteurs concernés par le phénomène du publipostage électronique : internautes, fournisseurs d'accès à internet, gestionnaires de services de messagerie électronique et de listes de diffusion, organismes de normalisation, professionnels du commerce et de l'édition de contenus électroniques, de la publicité électronique, de la vente à distance, etc.

Les organismes suivants ont répondu au courrier adressé par la CNIL afin de recueillir par écrit, après les avoir rencontrés, leurs observations : Eurocauce (Euro-coalition against unsolicited commercial e-mail), AFUTT (Association Française des Utilisateurs du Téléphone et des Télécommunications), UNAF (Union Nationale des Associations Familiales), AFA (Association des Fournisseurs d'Accès et de services Internet), CRU (Comité Réseaux des Universités), GESTE (Groupement des Editeurs de Services en ligne), AFTEL (Association Française de la Télématique Multimédia), IAB (Internet Advertising Bureau), FEVAD (Fédération des Entreprises de Vente à Distance), MEDEF (Mouvement des Entreprises de France), AFNOR (Association Française de Normalisation), la Chambre de Commerce Internationale (CCI).

L'étude du droit et des pratiques hors de l'Union européenne a fait ressortir en particulier qu'aux Etats-Unis la question était particulièrement préoccupante et faisaient l'objet de nombreuses initiatives y compris législatives. Ainsi, l'étude d'opinion réalisée par ATT en novembre 1998 a montré une nette augmentation du mécontentement des internautes américains. 52 % ont déclarés, en effet, que les prospections commerciales par e mail constituaient une gène sérieuse à l'utilisation d'internet contre 48 %, selon l'étude réalisée six mois auparavant par le professeur Alan Westin.

Les dispositifs mis en place aux Etats-Unis par les fournisseurs d'accès pour interdire la prospection commerciale électronique non sollicitée se sont avérés très vite inefficaces. Ces acteurs ont, dès lors, fait pression dans certains Etats, pour l'adoption de lois spécifiques « anti-spam », assorties de sanctions pénales. Ainsi plusieurs Etats ont déjà adoptés des législations dont le fondement a été recherché dans l'usage abusif par les « spammeurs », des moyens d'autrui, en l'occurrence des fournisseurs de services de messageries électroniques, en particulier les fournisseurs d'accès à internet. Ce fut le cas en 1999 en particulier des Etats de Washington, Californie, Névada. Au plan fédéral plusieurs projets de lois ont été également déposés.

C. A caractéristiques nouvelles, nouvelles garanties

1) UNE PROSPECTION À TRÈS FAIBLE COÛT POUR LE PROSPECTEUR

A 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 contenant jusqu'à 60 millions d'adresses électroniques (620 francs pour 2 millions d'adresses électroniques).

Quant aux frais de production et de diffusion des communications commerciales, ils sont dans le cas du publipostage électronique sans commune mesure — quelques centaines de francs — avec ceux générés par des envois postaux — fabrication d'une maquette, coût du papier, mise sous pli, affranchissement —, qui peuvent atteindre plusieurs dizaines de millions de francs. La prospection téléphonique, quant à elle, nécessite la mobilisation de personnels en grand nombre.

Ces données expliquent le développement de la prospection par télécopie durant des tranches horaires à tarif réduit (la nuit) ou le soutien que les professionnels ont apporté, dans un premier temps au moins, aux automates lanceurs d'appels et de messages commerciaux préenregistrés. Cependant, les abus ont été tels dans ces deux derniers domaines, que la CNIL, puis les professionnels eux-mêmes et, enfin, la réglementation européenne [1] ont subordonné l'usage d'automates d'appels et la prospection par télécopie à de fortes contraintes : un système de consentement exprès (*opt in*) dans les deux cas.

Plus le coût de la prospection est faible, plus les risques d'abus sont réels. C'est pourquoi plus le coût de la prospection est faible, plus les droits garantis aux personnes sont forts. Or, la prospection électronique est la moins coûteuse de toutes les formes de prospection existantes. Cette tendance lourde doit également faire partie de la réflexion.

2) UNE PROSPECTION ET UNE DIFFUSION COÛTEUSE POUR LES INTERNAUTES

L'internaute, qu'il lise ou non le message qui lui est adressé, supporte les frais de réception des messages induits par la récupération de courriers commerciaux non sollicités. Ainsi, un grand fournisseur d'accès déclarait, en mars 1999, recevoir 1,8 millions de « spams » par jour.

En admettant qu'un utilisateur moyen mette dix secondes pour rapatrier les messages qui lui sont destinés, le coût global pesant sur les abonnés de ce fournisseur d'accès recevant des « spams » peut être évalué à 90 000 francs par jour, à

1 Directives 97/66 du 15 décembre 1997 sur la protection des données personnelles dans le secteur des télécommunications et 97/7 du 20 mai 1997 sur la protection des consommateurs en matière de contrats à distance.

rapprocher des quelques centaines de francs que l'expéditeur du message aura utilisé pour entrer en contact avec les internautes.

3) UNE PROSPECTION « INTRUSIVE » ET DIRECTEMENT CIBLÉE

L'e-mail est une boîte aux lettres ouverte sur le monde et dépourvue des barrières que constituent, dans le monde physique, un hall d'entrée, un digicode, une gardienne.

L'e-mail est, par ailleurs, davantage personnalisée que ne l'est une boîte aux lettres physique ou la ligne téléphonique d'un domicile qui est généralement commune à plusieurs usagers.

Outre les sources d'informations classiques d'adresses, ici les e-mail, collectées par un responsable, directement auprès des internautes à l'occasion de leurs achats, internet ouvre potentiellement une source nouvelle d'informations particulièrement tentante pour les prospecteurs, sans précédent en quantité et qualifiant de manière nouvelle le profil des internautes concernés : les espaces publics d'internet sur tel ou tel sujet qui comportent les adresses électroniques des participants aux forums de discussion, les adresses électroniques de listes de diffusion accessibles au public, celles publiées dans le cadre d'annuaires particuliers accessibles sur internet.

D. Les recommandations de la CNIL

La Commission estime, au vu de ces éléments, qu'il convient de s'en tenir, au plan juridique, à tous les principes de protection des données à caractère personnel qui figurent dans la directive européenne du 24 octobre 1995 et à assurer leur effectivité.

Ainsi, dans le cas de la collecte de l'e mail directement auprès de la personne, il est déjà fait obligation à celui qui collecte des données d'informer la personne de la finalité du traitement des données, notamment de prospection, et de lui offrir la possibilité de s'y opposer.

De même lorsque l'internaute a été préalablement informé que son e-mail pouvait être cédé à des tiers, ou à des partenaires commerciaux, notamment à des fins de prospection commerciale, et a été mis en mesure de s'y opposer — par l'apposition d'une case à cocher — les fichiers ainsi régulièrement constitués peuvent être cédés et utilisés à de telles fins.

S'agissant de la collecte des e-mail dans espaces publics d'internet la CNIL estime, avec ses collègues européens, que de telles collectes ne peuvent être réalisées à l'insu des internautes et seraient contraires aux principes de la protection des données. Une telle collecte de donnée doit être considérée, en effet, comme déloyale au regard de l'article 6-1-a de la directive 95/46/CE, puisque la personne n'a pu en être informée au préalable. Elle est contraire au principe de finalité (article 6-1.b) parce que la personne qui a communiqué son e mail l'a fait à d'autres fins que celle de la prospection commerciale, par exemple en participant à un forum de discussion.

Ces recommandations ont été reprises par le groupe dit « de l'article 29 » dans son avis adopté le 3 février 2000 qui en outre reprend l'analyse de la CNIL sur la compatibilité de cette position avec l'ensemble des textes européens concernés par la prospection commerciale.

Cette compatibilité est en particulier assurée, grâce aux éclaircissements inscrits, à la demande du groupe dit « de l'article 29 », dans la directive relative à certains aspects du commerce électronique adoptée le 4 mai 2000 qui précise que les principes de la directive 95/46 sont applicables aux communications commerciales.

En outre, de manière à rendre effective la protection, la CNIL préconise des mesures pratiques en direction des acteurs concernés, telle la mise en œuvre par les sites d'une politique d'affichage systématique de l'interdiction d'utiliser à des fins de prospection à l'insu des internautes concernés et du responsable du site, les données personnelles diffusées pour une finalité déterminée. Cette politique peut inclure en outre l'insertion d'e-mail pièges (comme dans le monde réel) destinés à contrôler l'application de cette interdiction.

La Commission souhaite également promouvoir, en concertation avec les instances de normalisation de l'internet (IETF et W3C), des protocoles permettant aux responsables de sites d'interdire la collecte automatisée par le biais de moteurs de recherche de données personnelles figurant sur leur site. Dans le même esprit, la Commission s'assurera, en étroite liaison avec ses homologues européens et internationaux, que le projet de protocole P3P permettra aux internautes de s'opposer en ligne à la cession de leurs données à des tiers et d'exiger des sites qu'ils s'engagent à ne pas collecter les mails figurant dans des forums de discussion.

Enfin la Commission a souhaité encourager les chartes et les codes de bonne conduite des organismes professionnels qui s'engageront à interdire la collecte de données personnelles dans les espaces publics de l'internet à l'insu des personnes concernées.

La Commission, qui a procédé, dans le cadre de ce rapport, à une large consultation auprès d'associations d'internautes, de fournisseurs d'accès, de gestionnaires de messageries électroniques, d'associations et de syndicats professionnels ainsi que d'organismes de régulation et de normalisation se félicite de l'accueil reçu par ses positions.

Elle a pu constater par la suite, en effet, au cours de l'instruction de plaintes relatives à des prospections réalisées sur la base de collecte d'e-mail dans des espaces publics d'internet, que les acteurs concernés, informés de la position de la CNIL, ont déclaré prendre toute mesure pour que cesse ce mode de collecte de données.

GÉNÉRATION « TÉLÉCOMS »

L'année 1999 aura été celle de l'engouement pour le téléphone portable. Le nombre d'abonnés aux réseaux mobiles a quasiment doublé en une seule année passant de 12 millions en janvier 1999 à 21 millions en janvier 2000, nombre qui pourrait en moins de deux années rejoindre et dépasser celui des abonnés au téléphone fixe (33 millions de lignes).

Le maintien ou la conquête de parts de marchés des services de communication, désormais ouverts à la concurrence et sièges d'importantes innovations technologiques, lié à l'émergence d'une nouvelle génération de réseaux numériques de communication mobile permettant, notamment, l'accès à internet, conduit les opérateurs à concevoir de nouveaux services ou des offres tarifaires nouvelles.

Une série de services, dit de « communication avancée », commence à voir le jour, reposant en grande part sur l'utilisation par le réseau de notre numéro de téléphone comme une information à exploiter sous de nouvelles formes. Après la généralisation du service de présentation du numéro appelant, a été ouvert, en 1999, un autre de ces services, celui dit du dernier appelant.

Dans le même mouvement, sur la base de la donnée techniquement nécessaire qu'est la localisation d'un mobile, dont l'actualité judiciaire a révélé l'existence en France, les opérateurs envisagent d'offrir directement ou par l'intermédiaire de fournisseurs de services, des services de proximité fondés sur la localisation des mobiles. Jusqu'à présent cantonnée à un rôle purement technique et interne au réseau, cette donnée deviendrait l'objet d'une communication à des tiers.

Parallèlement, sur les réseaux mobiles, après l'offre d'un terminal téléphonique à 1 F en échange d'un contrat d'abonnement sur une longue période, la communication gratuite apparaît, en contrepartie de l'acceptation que nos conversations téléphoniques soient interrompues par un ou plusieurs messages publicitaires.

La Commission s'est attachée à étudier de la manière la plus précise les mécanismes mis en œuvre dans tous ces services, à évaluer les risques et à peser sur les évolutions de manière à promouvoir, ou faire émerger, d'une part, auprès des opérateurs, des choix conciliant convivialité et protection de la vie privée, d'autre part, auprès des pouvoirs publics, des solutions conciliant protection de la vie privée et impératifs de l'ordre public. L'enjeu est clair : éviter que les nouvelles technologies associées à la société de communication ne constituent, à notre insu, un des pièges de nos sociétés modernes et les transforment « malgré elles », en sociétés de surveillance.

I. LA LOCALISATION DU TÉLÉPHONE PORTABLE

La Commission a procédé en mai — juin 1999, en concertation avec les trois opérateurs de réseaux de communications mobiles, Bouygues Télécom, France Télécom et SFR, à une étude approfondie des conditions techniques dans lesquelles les informations permettant la localisation des terminaux mobiles sont aujourd'hui traitées, de leurs évolutions possibles et de leurs incidences en termes de libertés.

Le résultat de cette étude montre, au-delà de la complexité technique de ces réseaux, fonctionnant actuellement selon les normes GSM 900 et DCS 1800 et qui s'appuient pour partie sur des infrastructures de commutation téléphonique, c'est-à-dire sur du réseau fixe, et pour partie sur des infrastructures radio, qu'il y a lieu d'une part de relativiser certaines craintes parfois émises, mais aussi de tenir compte de l'émergence de nouveaux services fondés sur la localisation et de répondre à deux problèmes.

A. Quelques données techniques

Un téléphone portable éteint n'est localisable en aucune façon. Tout au plus, connaît-on la zone géographique dans laquelle se trouvait le portable lorsqu'il a été éteint.

Lorsque le téléphone est en veille, il est repéré dans le réseau au niveau central par l'indication du centre de commutation dont il est le plus proche (chaque opérateur dispose de 40 centres environ répartis sur le territoire) et au niveau de ce commutateur par l'indication de la zone radio dans laquelle se trouve la cellule à laquelle il s'est « accroché ». Cette zone dite « zone LAC » (Location Area Cell) correspond à une zone géographique d'une taille variable et qui peut être, selon le cas, équivalente à celle d'un quartier de grande ville, à la taille d'une petite ville ou, lorsque la zone est peu peuplée, d'un département.

Au fur et à mesure que se déplace le détenteur d'un mobile, les informations contenues dans les équipements du réseaux sont mises à jour automatiquement et

aucun historique des mises à jours successives ou « déplacements » n'est conservé ni au niveau central, ni au niveau des centres de commutation.

Lorsqu'un appel est émis ou reçu par un téléphone portable, un compte rendu d'appel ou « CRA » est transmis par le centre de commutation qui gère l'appel vers la chaîne de traitements destinée à la facturation. Ce compte rendu d'appel comporte, outre l'identification des numéros appelant et appelés, la date, l'heure du début de la communication et sa durée — comme pour la téléphonie fixe — l'indication, selon un code interne à l'opérateur, de la cellule de départ de la communication. C'est cette information suppémentaire qui permet de nous localiser, appel par appel.

B. La localisation de nos appels est concernée

Cette donnée de localisation relative à la cellule d'où un appel est émis ou reçu, la plus fine possible dans un réseau de communication mobile, n'est pas portée sur la facture remise au client. Elle n'est pas davantage accessible aux services en relation avec la clientèle. Mais elle est conservée par les opérateurs et selon des durées variables.

Ainsi, France Télécom conserve cette donnée de localisation, au même titre que les autres données liées à la facturation, durant un an — délai fixé par l'article L.126 du code des P et T pendant lequel la facture peut être contestée — mais les deux autres opérateurs, qui ne sont pas tenus par les termes de cet article du code des P et T conservent la donnée de localisation au même titre que les autres données liées à la facturation de 18 mois à trois ans pour répondre à d'éventuelles contestations. Interrogés par la CNIL, les trois opérateurs reconnaissent cependant que les cas dans lesquels la localisation de l'appel a dû être invoquée au titre d'une contestation de facture sont très marginaux.

Un autre motif de conservation de cette donnée de localisation est avancé par les opérateurs qui peuvent souhaiter adapter leurs tarifs en fonction de la zone de couverture de l'appel, les appels passés dans une même zone géographique pouvant bénéficier de tarifs plus avantageux. L'information liée à la localisation géographique des appels serait donc nécessaire pour appliquer ces tarifs adaptés.

Enfin, et ce point n'est pas négligeable, les opérateurs sont de plus en plus fréquemment saisis de demandes d'accès à l'information de localisation d'un appel dans le cadre d'enquêtes de police judiciaire. La police judiciaire, dans ce cadre, peut rechercher, non seulement comme cela se fait pour la téléphonie fixe, la liste des numéros ayant été appelés, et à quel moment, par une personne suspectée d'un crime ou d'un délit, mais aussi, puisque cela est désormais possible, le lieu où se trouvaient l'appelant et l'appelé au moment de l'appel. Il peut advenir aussi que la police souhaite disposer, dans le cadre de son enquête de l'ensemble des messages d'appels passés dans une zone géographique déterminée, afin de pouvoir exploiter à des fins d'identification criminelle l'ensemble des données du trafic téléphonique de cette zone. Les demandes présentées dans le cadre d'une enquête de police judiciaire ou d'une instruction judiciaire se rapportent généralement, aux dires des opérateurs, à des événements datant de moins de six mois. C'est cependant pendant des

durées beaucoup plus longues (le double, le triple, voire le quadruple) que cette information est actuellement conservée.

C. L'émergence de nouveaux services

Tous les opérateurs cherchent à développer des services, liés à la « mobilité », qui reposent sur la localisation des portables. Pour l'heure, chaque opérateur dispose de l'indication de la zone de localisation du téléphone portable selon un code interne, non opposable et non connu des autres opérateurs. Aussi, ce défaut d'inter-opérabilité limite-t-il pour l'heure les services qu'ils développent.

Il pourra s'agir du routage des appels vers le service d'urgence le plus proche du téléphone portable, ou le plus proche du centre d'appel délocalisé d'une entreprise disposant d'un numéro d'appel national. Il peut également s'agir du service qui peut être rendu à un particulier souhaitant savoir quel est le restaurant le plus proche de la zone où il se trouve, il peut s'agir aussi d'une compagnie de taxis souhaitant pouvoir convoyer celui des taxis qui se trouve dans la zone la plus proche du téléphone portable appelant.

Enfin, il est loin d'être exclu qu'à terme la localisation géographique de l'appelant soit transmise, c'est-à-dire affichée sur l'écran de la personne appelée comme peut l'être, à l'heure actuelle, le numéro de la ligne appelante**.**

D. Les questions vives

La conservation de la localisation de nos appels et la disparité constatée des durées de conservation, d'un opérateur à l'autre, est préoccupante.

Sur ce point la directive européenne 97/66 du 15 décembre 1997, sur la protection de la vie privée et des données personnelles dans le secteur des télécommunications a précisé les choses. Les données de trafic (y compris donc celle de la localisation d'un téléphone portable) doivent être effacées dès la fin de la communication. Une exception est prévue : les données nécessaires à la facturation peuvent être conservées durant la période pendant laquelle la facture peut être contestée, mais doivent être effacées ensuite. L'absence d'harmonisation, au plan national, de la durée pendant laquelle les données de facturation peuvent être conservées par les opérateurs est regrettable.

Ainsi, la Commission a-t-elle souhaité que la transposition de cette directive soit l'occasion d'harmoniser les durées de conservation et de les fixer dans un maximum qui pourrait être le délai déjà prévu par l'article L.126 du code des P et T, soit un an. La localisation de nos appels pourrait ainsi être conservée pendant un délai non exorbitant du droit commun et de nature à concilier impératifs d'ordre public et liberté d'aller et venir. Ce délai, malgré tout assez long, mais justifié par le motif de la facturation ne devra pas cependant être confondu avec celui qu'il conviendra également de fixer lié aux données de connexion à internet qui sont d'une autre nature et dont la conservation n'est pas motivée par la préoccupation de la

facturation appel par appel du service. En effet, l'accès à internet donne lieu en général, lorsqu'il n'est pas gratuit, à un paiement forfaitaire.

Il est par ailleurs essentiel de veiller aux incidences du développement de services dits de « proximité » qui conduiront à moyen terme les opérateurs à offrir la présentation à l'appelé de la localisation de l'appelant. Serait-il légitime que toute utilisation de téléphone portable révèle à notre interlocuteur le lieu géographique d'où nous lui téléphonons ?

La Commission a souhaité que soit examinées, préalablement à l'ouverture de tels services, les possibilités techniques permettant à toute personne de s'opposer à la transmission de cette information à un tiers, une telle opposition devant pouvoir être levée, soit de manière systématique vis-à-vis des services d'urgence, soit de manière ponctuelle et au choix de l'appelant en fonction du service ou de la personne appelée.

Sur ces deux points, la position de la CNIL a rencontré un très large écho lors de la conférence annuelle des commissaires à la protection des données qui s'est tenue à Hong Kong les 13-15 septembre 1999, et la Commission européenne a manifesté son intention de réglementer cette matière dans le cadre de la mise à jour de la directive 97/66. Affaire à suivre donc, mais sans tarder si l'on souhaite que les exigences de la protection des données soient prises en compte dès le moment de la conception et de la commercialisation des services, à l'heure où la diffusion du langage WAP pour l'accès à internet par téléphone portable devrait favoriser l'émergence très rapide notamment de services fondés sur la localisation.

II. LOCALISATION PAR GPS

Une localisation plus fine (à quelques dizaines de mètres près) que celle obtenue avec les réseaux de communication mobile de type GSM peut d'ores et déjà être réalisée par GPS. Le système de localisation par « GPS » (*global positionning system*) mis en place par le ministère américain de la Défense est le premier qui ait été ouvert au public. Ce système connaît actuellement une grande vogue, compte tenu de la baisse des prix des récepteurs : on en trouve aujourd'hui pour moins de 1000 F.

La Commission a, au-delà des contacts qu'elle a pu avoir avec des sociétés envisageant d'utiliser ce système de navigation, examiné, pour la première fois en 1999, un service proposé par un constructeur automobile, le service ODYSLINE proposé par la Régie Renault, faisant appel à cette technologie de localisation associée à celle du GSM.

A. Quelques données techniques

Le GPS est un système de radionavigation qui permet 24 heures sur 24, à n'importe quel utilisateur équipé d'un récepteur de connaître sa position en trois di-

mensions (longitude, latitude, altitude), sa vitesse, ainsi que l'heure universelle (dite UTC [1], pour « temps universel coordonné »). Cette position est calculée par le récepteur de l'utilisateur à partir du croisement des informations en provenance d'au moins trois des satellites du système NAVSTAR (*navigation system time and ranging*) composé d'une flotte de vingt-quatre satellites installés quatre par quatre sur six orbites circulaires différentes, à 20 000 km de la Terre. Chaque satellite effectuant une révolution complète autour de la Terre en douze heures, de cinq à huit satellites sont à tout moment « en vue » d'un éventuel utilisateur muni d'un récepteur GPS.

Les satellites sont suivis et contrôlés au sol par un système de contrôle opérationnel composé d'un centre de contrôle principal et de cinq stations de contrôle dites « passives » dans la mesure où elles constituent des récepteurs d'informations en provenance des satellites qu'elles transmettent au centre de contrôle. C'est le cœur du GPS.

Chaque satellite émet en permanence, grâce aux informations transmises par le centre de contrôle terrestre, sa position et l'heure précise UTC. Grâce à son horloge interne, le récepteur GPS mesure le temps que met le signal du satellite pour lui parvenir. Le récepteur GPS doit mesurer les signaux émis par au moins trois satellites « en vue » et procéder à une triangulation à partir de ces données pour déterminer sa position en deux dimensions (longitude et latitude), et par quatre satellites pour une position en trois dimensions (longitude, latitude et altitude).

NAVSTAR recouvre en réalité deux systèmes différents : le premier (*precise positioning system*, ou PPS) reste réservé aux forces militaires américaines et alliées, ainsi qu'à certains organismes étatiques américains, tandis que le second (*standard positioning service*, ou SPS) est ouvert à tous. La principale différence entre les deux systèmes concerne la précision des mesures fournies à l'utilisateur, le premier — comme son nom l'indique — étant plus précis que le second.

Enfin, il convient d'insister sur le fait que le récepteur de l'utilisateur ne transmet aucune information aux satellites « en vue ». Ce sont ces derniers qui émettent un signal radio qui sera interprété par le GPS de l'utilisateur.

B. Les utilisations possibles et envisageables du GPS

Employé seul ou en combinaison avec d'autres applications technologiques, les utilisations du GPS sont multiples, des plus évidentes (navigation, bien entendu) aux plus insoupçonnées (surveillance des mouvements des plaques tectoniques, suivi et étude des rhinocéros en Afrique du Sud, mesure de parcelles agricoles…).

Utilisé seul, le GPS permet à un utilisateur de connaître à tout moment sa position. Déjà utilisé par la navigation maritime et aérienne, ainsi que lors de certaines épreuves sportives de type « raid » (Paris-Dakar, par exemple), l'usage des

1 Le temps universel coordonné (UTC), compromis entre le temps universel corrigé (UT I) et le temps atomique international (TAI), est l'échelle de temps commune aux diffusions des signaux horaires. Il est à la base du temps en usage dans tous les pays. Les horloges maîtresses des laboratoires horaires réalisent pratiquement l'UTC à quelques centaines de nanosecondes près.

récepteurs GPS, du fait de leur miniaturisation et de la baisse des prix, s'ouvre aux randonneurs et aux chasseurs (notamment dans le grand Nord canadien).

Couplé à un ordinateur disposant d'une base de données cartographiques, le système permet de « traduire » les informations relatives à la longitude, latitude et altitude du récepteur GPS en un point sur la carte d'une région ou d'une ville ainsi que de déterminer l'itinéraire optimal d'un point à un autre.

On notera à ce propos que la précision du GPS étant insuffisante, notamment en milieu urbain, les applications d'aide à la navigation intègrent une fonction de « localisation du véhicule » qui repose sur l'évaluation de la position de la voiture grâce aux informations transmises par des capteurs situés dans les roues, et la correction de ces informations par une corrélation instant par instant entre le parcours estimé et les cartes du réseau routier digitalisées à bord. Cette opération de positionnement, faite automatiquement par le récepteur GPS du véhicule, est précise à dix mètres près.

Ces dispositifs, parfois secondés par une application de synthèse vocale, entrent dans la catégorie des systèmes d'aide à la navigation embarqués. Ils présentent toutefois un inconvénient : La technique — même la plus sophistiquée — est parfois moins rapide que les hommes : en France 20 % des panneaux et des carrefours changent chaque année, ce qui rend les cartes assez rapidement obsolètes !

Couplé à un réseau radio (celui utilisé par les téléphones mobiles, par exemple), le système permet à des organismes (transports en commun) ou des entreprises (compagnies de taxis, loueurs de voitures, transporteurs routiers) de localiser en temps réel, 24 heures sur 24, l'ensemble des véhicules de leur flotte afin d'optimiser la gestion de leur parc.

Certains systèmes de ce type sont déjà en fonctionnement, qu'il s'agisse d'entreprises de transports en commun ou de sociétés privées. Ainsi, le système AIGLE, mis en œuvre localement à titre expérimental par la RATP depuis novembre 1994, facilite le traitement des alarmes liées à la sécurité des biens et des personnes de l'ensemble des réseaux RATP. Il s'appuie essentiellement sur un système de radiolocalisation des véhicules fondé sur l'observation par satellites. Une cinquantaine de véhicules d'intervention sont aujourd'hui équipés d'un boîtier de radiolocalisation qui permet au « central » de connaître en temps réel la position des bus à dix mètres près. Les deux mille véhicules de la société des Taxis bleus sont équipés d'un GPS de façon à ce que la « centrale » sache à tout moment où se trouve chaque voiture (optimisation des temps de déplacements, réduction du temps d'attente des clients).

Enfin, si l'on ajoute à l'ordinateur qui gère à la fois le récepteur GPS et la base de données cartographiques un système d'exploitation des informations relatives au trafic (reçues par radio, ces informations sont décodées par l'ordinateur de bord et intégrées à la base de données cartographiques, permettant une mise à jour quasi instantané), on dispose d'un véritable outil d'aide à la circulation qui permet notamment d'éviter travaux, bouchons, etc., signalés en temps réel au conducteur.

Certaines applications de ce type sont déjà proposées, au nombre des options, par certains constructeurs automobiles et certains équipementiers.

Le service que Renault SA a déclaré à la CNIL, relève de cette dernière catégorie.

C. Un cas concret examiné par la CNIL

Renault a soumis à l'examen de la CNIL un service d'assistance associant le système GPS et le réseau GSM reposant sur un ordinateur embarqué qui transmet automatiquement à une plate — forme d'assistance téléphonique ou médicale des informations concernant le véhicule de l'abonné et, singulièrement, sa position géographique.

Dans le véhicule, l'utilisateur dispose pratiquement de trois boutons (rouge, orange et vert) reliés à un boîtier télématique, le boîtier étant lui-même relié à un capteur de choc, à un récepteur GPS — qui sert à localiser le véhicule — et à un téléphone relié au réseau GSM. C'est par l'intermédiaire de ce dernier (appel automatique, en cas de choc, ou appel volontaire de l'abonné) que sont transmis à la plate-forme d'assistance le numéro de téléphone de l'abonné — qui permet de l'identifier —, la position du véhicule et la nature de l'appel.

La transmission d'informations à la plate-forme d'assistance ne peut être effectuée qu'à partir du véhicule ; en aucun cas, la plate-forme ne peut connaître la localisation du véhicule lorsque le GSM est seulement en veille, sans intervention de l'abonné ou en l'absence de détection d'un choc.

Deux aspects de ce dossier ont retenu l'attention de la Commission, celui de l'information préalable de l'abonné à ce service et celui de la durée pendant laquelle les informations relatives à la localisation sont conservées par le service.

Sur le premier point, la Commission a demandé que soit précisée la mention d'information figurant dans le contrat d'abonnement à ce service : elle apparaît désormais à la fois très complète et très explicite. En particulier une précision est apportée à destination des personnes ayant opté pour le secret du numéro de leur téléphone portable les informant que le système ne fonctionne qu'à partir de l'identification de leur numéro de téléphone et donc de l'outrepassement de la fonction « secret ». En effet, seul le numéro de téléphone portable associé au véhicule peut identifier le client. En outre, les personnes sont informées, conformément aux dispositions de l'article 27 de la loi du 6 janvier 1978, que les données peuvent être communiquées à des tiers et qu'elles peuvent s'opposer à cette transmission en cochant une case prévue à cet effet selon la doctrine de la Commission.

La durée pendant laquelle les informations peuvent être conservées par Renault était l'autre élément important du dossier. Localiser le véhicule au moment où l'abonné à ce système le sollicite est une chose ; la durée pendant laquelle la plate-forme va conserver les informations relatives à cette localisation en est un autre.

Les coordonnées d'un véhicule équipé du système prennent, lors de l'appel, la forme, pour les opérateurs de la plate-forme d'assistance, d'un indicateur lumineux apparaissant sur une carte routière à l'endroit exact où se trouve l'abonné. Au-delà d'un délai d'une heure, seules apparaissent les coordonnées géographiques du

véhicule — sous la forme d'une longitude et d'une latitude ; elle ne sont alors plus accessibles qu'au responsable de la plate-forme et à l'informaticien chargé du service.

En revanche, les informations relatives à la localisation du véhicule sont conservées pendant de longues durées et différentes selon la nature de l'appel : 10 ans pour les appels d'urgence, 5 ans dans les deux autres cas.

Renault a justifié de telles durées en précisant que sa responsabilité civile pourrait se trouver engagée en cas d'impossibilité d'administrer tous les éléments nécessaires à la preuve du bon fonctionnement du service. L'argument ne manque pas de force juridique. Il soulève cependant la question d'ordre général de l'adaptation des durées de prescription de l'action civile en responsabilité contractuelle ou délictuelle dans une société numérique.

III. APPEL ET RAPPEL

France Télécom a adressé le 18 février 1999 une déclaration ordinaire préalablement à l'ouverture commerciale d'un nouveau service dénommé « 3131, Rappel du dernier appelant » qui a été ouvert en septembre 1999. Ce service repose sur la mémorisation dans le réseau du numéro appelant lorsque l'appel est demeuré sans réponse.

France Télécom aura été le second opérateur de téléphonie fixe en Europe, après British Telecom, à offrir de manière générale ce service, très répandu aux USA, qui fait partie des services dits de « communication avancée » qui comprennent outre la présentation du numéro appelant, la transmission du nom de l'abonné de la ligne appelante, le refus des appels non identifiés par le numéro de téléphone appelant « *block blocking* », la présentation à l'appelant du numéro de téléphone avec lequel il se connecte « *connected line* ». Ces derniers services ne sont pas ouverts encore en France, certains devront faire, à l'évidence l'objet d'un examen particulier.

Offert gratuitement à tout abonné, le service du rappel du dernier appelant permet de rappeler automatiquement le dernier correspondant auquel l'abonné n'a pas répondu en composant le numéro 3131. Un message vocal indique alors la date, l'heure et le numéro de téléphone du dernier appel. L'appelé peut alors, s'il le souhaite, déclencher le rappel automatique de ce numéro en composant le 5.

Pour des motifs évidents, le service ne concerne pas les utilisateurs, appelants ou appelés, des publiphones, points phone, et services de téléphone à cartes. Il ne concerne pas non plus les abonnés qui ont souscrit au service de présentation du numéro appelant (plus d'un million) dont le terminal est doté d'un enregistreur des appels, ni les abonnés qui disposent d'un répondeur, lorsqu'il est branché, puisque par définition, dans ce cas-là l'appel est « pris ». Il n'en demeure pas moins que ce service concerne environ 50 % des abonnés.

Evidemment le caractère automatique d'un tel service, qui peut d'emblée être utilisé depuis tous les postes, même par des personnes qui auraient pu souhaiter

ne pas en disposer, peut être de nature à attirer des curiosités aux conséquences parfois incertaines sur la paix des familles… ou des ménages.

Conscient de ces inconvénients, France Télécom a prévu diverses mesures de précaution ou de protection de la vie privée.

En premier lieu, seul le numéro du dernier appelant est enregistré. Ce numéro sera conservé jusqu'à ce qu'il ait été rappelé ou jusqu'à ce qu'un nouvel appel vers le même correspondant demeure sans réponse, la mémorisation du numéro de téléphone correspondant à ce nouvel appel effaçant systématiquement le numéro de téléphone précédemment enregistré. Il est estimé qu'en moyenne le numéro du dernier appelant ne sera pas conservé au-delà d'une période de 5 jours.

En deuxième lieu, tout abonné peut effacer automatiquement le numéro enregistré, sans avoir à l'appeler, en composant la séquence suivante #92#. Il convient d'observer que cette solution technique est actuellement à l'étude par British Telecom, à la demande du commissaire à la protection des données du Royaume-Uni, pays où un tel service est ouvert depuis plusieurs années, sans qu'une telle mesure ait été prévue.

En troisième lieu et surtout, tout abonné peut demander en s'adressant à son agence, à renoncer au service. Dans ce cas, le numéro du dernier appelant ne sera jamais mémorisé. Encore convient-il d'entreprendre une démarche auprès de France Télécom.

Enfin, en aucun cas le numéro d'appel d'une personne ayant demandé que son numéro ne soit pas transmis à l'appelant dans le cadre du service de présentation du numéro appelant ne sera enregistré. On se rappellera, à cet égard, que tout abonné a la possibilité de demander que son numéro ne soit pas divulgué dans le cadre du service de présentation du numéro appelant soit de manière permanente, soit appel par appel en composant le numéro 3651 avant de composer le numéro de son correspondant.

Après 16 mois de la généralisation de l'offre du service de la présentation du numéro appelant 1 100 000 personnes ont opté pour le secret permanent.

Il est à noter que France Télécom a effectué une campagne d'information très importante au cours des mois de juillet et d'août 1999 dans le cadre de « la lettre de France Télécom » qui est adressée à ses abonnés avec leur facture ainsi que par voie de presse et de radio. A cet égard, et conformément au vœu exprimé par la CNIL lors de la mise en place du service de présentation du numéro appelant, France Télécom a retenu le principe, d'une information équilibrée présentant tant le service que l'ensemble des moyens de protection.

Ainsi, l'ouverture de ce service n'a-t-il généré que très peu de plaintes ou de réclamations.

IV. INTERRUPTIONS PUBLICITAIRES

La CNIL a examiné, lors de sa séance du 5 octobre 1999, les problèmes soulevés par les projets de certains opérateurs de téléphonie qui consistent à offrir une baisse des tarifs de communications téléphoniques en contrepartie de l'acceptation par l'abonné que ses communications téléphoniques puissent être interrompues par des messages publicitaires.

La CNIL a relevé le caractère inédit en France de l'utilisation de correspondances privées comme support d'annonces publicitaires et a souligné qu'à la différence des offres de connexion gratuite à Internet, la contrepartie de ces tarifs préférentiels en matière de téléphonie ne pesait pas uniquement sur celui qui y avait consenti mais aussi sur ses interlocuteurs, les personnes appelées.

Relevant qu'en l'état actuel du droit, aucun texte de caractère national ou international n'interdisait de telles offres, la Commission a cependant souhaité rappeler à l'ensemble des opérateurs français les règles minimales de préservation de la vie privée et de la tranquillité que devaient respecter les projets de cette nature, tant au regard de la loi « informatique et libertés » que des dispositions relatives à la liste orange.

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.

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.

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.

Les numéros de ligne 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).

Bouygues Télécom est le premier opérateur a avoir ouvert commercialement un tel service en avril 2000 reposant sur une carte de téléphone portable prépayée comportant une zone rechargeable d'unités gratuites moyennant l'interruption de spot publicitaire. La mise en œuvre de ce service respecte les recommandations élaborées par la CNIL et qui ont été portées à la connaissance de l'ensemble des opérateurs.

SANTÉ ET PROTECTION SOCIALE : DES QUESTIONS DE PLUS EN PLUS SENSIBLES

Longtemps, l'information ne s'est échangée qu'entre le malade et son médecin, puis la médecine est passée de l'oral à l'écrit. L'information demeurait cependant encore consignée dans le dossier médical, accessible au seul médecin traitant. L'évolution de la pratique médicale et la généralisation du système de protection sociale ont contribué à élargir au fil du temps « le cercle des confidents nécessaires » : médecins spécialistes, équipes soignantes, médecins conseils... Qu'il s'agisse des systèmes d'information hospitaliers, des réseaux de soins ville — hôpital, des messageries médicales, de la télétransmission via le Réseau Santé-Social (ou d'autres réseaux) des feuilles de soins électroniques, de la télémédecine, des réseaux de recherche médicale, les données de santé ont aujourd'hui vocation à s'échanger non seulement entre les professionnels de santé eux-mêmes mais également avec l'ensemble des acteurs du système de soins : caisses de sécurité sociale, organismes de tutelle, INSERM, laboratoires pharmaceutiques...

Trois facteurs, au moins, favorisent une telle évolution :

Les progrès constants de la médecine induisent une pratique médicale de plus en plus spécialisée, et donc un nécessaire partage du savoir et de l'information entre les professionnels de santé.

Le contexte actuel de maîtrise des dépenses de santé est propice à une gestion plus rationnelle du système de protection sociale et une connaissance plus fine de l'état de santé de la population et des pratiques médicales, ce qui nécessite le recours à des outils modernes de traitement de l'information.

La banalisation de la micro informatique, les capacités sans cesse accrues de stockage et de traitement des données, et surtout le développement du réseau internet et des outils de messagerie, incitent naturellement à une multiplication des échanges d'informations dans le monde de la santé.

Mais dès lors qu'il s'agit d'informations couvertes par le secret médical, comment concilier le droit de chacun au respect de l'intimité de sa vie privée, l'indispensable confidentialité des données de santé et le besoin ressenti d'un accès plus large à l'information médicale, y compris de la part des usagers eux mêmes ?

Au cours de ces derniers mois, trois dossiers d'actualité ont relancé la réflexion sur le sujet. Le premier concernait la mise en place des déclarations obligatoires de séropositivité au VIH ; le deuxième, évoqué en incidente des débats parlementaires sur la couverture maladie universelle, les conditions de diffusion, notamment à la presse, de données sur l'activité hospitalière ; le troisième le déploiement sur l'ensemble du territoire, du dispositif SESAM VITALE.

I. LA DÉCLARATION OBLIGATOIRE DES CAS DE SÉROPOSITIVITÉ

A la suite des débats intervenus sur les modalités de la mise en place de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine (VIH), la CNIL a décidé de mener une réflexion d'ensemble sur le dispositif de surveillance épidémiologique de cette affection. La CNIL a notamment consulté différentes associations de défense des malades atteints du sida, la Ligue des droits de l'homme et le Conseil national de l'Ordre des médecins. Elle a, en outre, recueilli sur place l'avis de médecins inspecteurs des directions départementales des affaires sanitaires et sociales. Enfin, elle s'est rendue dans les locaux de l'Institut de Veille Sanitaire, chargé notamment de la surveillance épidémiologique du sida, afin de se rendre compte concrètement de son action et des mesures de confidentialité adoptées. La situation chez la plupart de nos voisins européens a également été étudiée.

Rappel du contexte

Au cours du printemps 1998, le Ministre de la Santé annonce officiellement la décision d'inscrire la séropositivité au virus de l'immunodéficience humaine parmi la liste des maladies à déclaration obligatoire.

Un décret du 6 mai 1999, pris en application de la loi du 1er juillet 1998 sur la veille sanitaire, inscrit dans la liste des maladies à déclaration obligatoire l'infection par le virus de l'immunodéficience humaine, quelque soit le stade de l'infection.

Un autre décret daté du même jour suscite au cours de l'été 1999 de nombreuses réactions de la part d'associations de patients, relayées par la presse. Celles-ci redoutent que ce texte permette la mise en place d'un « fichage » nominatif des personnes séropositives et, dès lors, s'inquiètent de l'avenir d'un dépistage anonyme. En effet, alors que la loi du 1er juillet 1998 dispose que « les modalités de la transmission des données à l'autorité sanitaire..., en particulier la manière dont l'anonymat est protégé, sont fixées par décret en Conseil d'Etat », le décret prévoit que la notification des déclarations est réalisée « sous la forme d'une fiche qui

comporte des éléments à caractère nominatif », ce qui peut donner à penser que les données transmises seraient directement nominatives.

Parallèlement, l'Institut de Veille Sanitaire (IVS) saisit la CNIL, en mars 1999, d'une demande d'avis relative à l'expérimentation, dans vingt-deux départements, d'un traitement informatique des déclarations obligatoires de séropositivité.

Comme c'est le cas pour les cas de sida déclaré, il est envisagé que les déclarations soient transmises sous pli confidentiel au médecin inspecteur de la DDASS, à charge pour ce dernier de valider les données, et de les adresser, sous pli confidentiel au médecin épidémiologiste chargé de la surveillance du VIH à l'IVS. Les déclarations doivent comporter outre les données médicales, les initiales du nom et les initiales du prénom, le sexe, la date de naissance, la nationalité, le département ou pays de résidence, le code postal de domicile et le code INSEE de la catégorie socio-professionnelle, le mode de transmission présumé et le pays d'origine du partenaire en cas de contamination hétérosexuelle probable. Enfin le nom du médecin déclarant et son lieu d'exercice ainsi que la date de déclaration doivent également y figurer. La CNIL demande alors des précisions sur les modalités de transmission des informations et les dispositions prises pour assurer leur confidentialité. La polémique suscitée par la parution du décret la conduit à faire paraître en juillet 1999 un communiqué de presse rappelant qu'aucun avis n'a encore été rendu et qu'en conséquence aucun traitement automatisé ne peut être mis en œuvre par l'Institut de veille sanitaire.

Le ministre décide alors de suspendre le projet et de constituer avec les associations de patients un groupe de travail chargé de réexaminer les modalités de mise en place du dispositif des déclarations obligatoires, tant en ce qui concerne leur contenu que les procédures de déclaration et d'éventuelles solutions techniques d'anonymisation. En outre, il est annoncé que le décret du 6 mai 1999 sera modifié. Parallèlement, la CNIL décide, par délibération du 9 septembre 1999, qu'il y a lieu en l'état de différer l'examen de la demande d'avis présentée par l'Institut de Veille Sanitaire et d'entreprendre une étude d'ensemble sur cette question afin de pouvoir faire part aux pouvoirs publics de ses conclusions et en particulier de l'opportunité ou non de disposer d'informations individuelles.

Délibération n° 99-042 du 09 septembre 1999 relative à une demande d'avis présentée par l'institut de veille sanitaire concernant la mise en place à titre expérimental des déclarations obligatoires de séropositivité au virus de l'immunodéficience humaine

La Commission Nationale de l'Informatique et des Libertés,

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 traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la Convention nº 108 du Conseil de l'Europe du 28 janvier 1981 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'Informatique, aux fichiers et aux libertés ;

Vu la loi nº 98-535 du 1er juillet 1998 relative au renforcement de la veille sanitaire ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 ;

Vu le décret nº 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 L11 du code de la santé publique ;

Vu le décret nº 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 ;

Après avoir entendu Monsieur Raymond FORNI en son rapport et Madame Charlotte-Marie PITRAT en ses observations ;

Considérant que l'Institut de Veille Sanitaire, organisme chargé de la surveillance épidémiologique du sida a saisi la CNIL d'une demande d'avis relative à la mise en place, à titre expérimental dans vingt-deux départements, d'un traitement automatisé des déclarations obligatoires de séropositivité au virus de l'immunodéficience humaine ;

Considérant que deux décrets du 6 mai 1999 pris en application de la loi du 1er juillet 1998 susvisée ont d'une part inscrit dans la liste des maladies à déclaration obligatoire l'infection par le virus de l'immunodéficience humaine, quelque soit le stade de l'infection et d'autre part prévu la transmission à l'autorité sanitaire de données individuelles ;

Considérant que les informations collectées et destinées à être traitées sur support informatique par l'Institut de Veille Sanitaire dans le cadre de l'expérimentation envisagée sont : les initiales du nom et du prénom, le sexe, la date de naissance, la nationalité, le département ou pays de résidence, le code postal de domicile et le code Insee de la catégorie socio-professionnelle ; que sont également collectées des données propres à caractériser l'infection, le nom du médecin déclarant et le lieu d'exercice ainsi que la date de déclaration ;

Considérant que l'expérimentation et la mise en place du dispositif de surveillance des déclarations obligatoires de séropositivité au virus de l'immunodéficience humaine sont suspendues à l'initiative du Ministère en charge de la santé afin notamment de procéder à un réexamen des différentes modalités du dispositif en concertation avec les associations de patients ;

Considérant qu'il y a lieu en l'état pour la Commission de différer l'examen de la demande d'avis présentée par l'Institut de Veille Sanitaire ;

Constate qu'il y a lieu de différer en l'état l'examen de la demande d'avis présentée par l'Institut de Veille Sanitaire jusqu'à ce que cet institut décide de mettre en œuvre à titre expérimental ou définitif le dispositif de surveillance des déclarations obligatoires de séropositivité au virus de l'immunodéficience humaine tel qu'il sera arrêté.

A. Les fichiers épidémiologiques

L'épidémiologie a pour objet d'étudier la fréquence et la répartition de problèmes de santé en termes de morbidité et de mortalité en fonction de leur évolution dans le temps, de leur localisation géographique, des caractéristiques démographiques, et de rechercher les facteurs de risque et les causes des maladies. La poursuite de ces objectifs peut donc nécessiter la collecte d'informations sur les personnes et la constitution de fichiers pour certains anonymes, pour d'autres directement ou indirectement nominatifs.

1) LES DIFFÉRENTS MODES DE RECUEIL D'INFORMATIONS

Le problème posé est celui de savoir si la qualité, la fiabilité et la validité scientifique des analyses statistiques doit conduire à préférer un système privilégiant une collaboration volontaire ou conduire à un système qui ferait obligation aux médecins et aux patients de communiquer les informations nécessaires.

En France, les fichiers épidémiologiques sont généralement institués sur la base d'une participation volontaire des professionnels de santé, la loi n'imposant aux médecins de transmettre des informations sur leurs patients que dans un nombre très limité de situations.

Le constat est le même s'agissant du patient, le droit français privilégiant en ce domaine les libertés individuelles. Le droit de s'opposer à l'utilisation de ses données à des fins de recherche médicale a d'ailleurs été consacré par la loi du 1er juillet 1994 qui a complété sur ce point la loi du 6 janvier 1978.

Ainsi, si l'on excepte les rares enquêtes de santé obligatoires menées par l'INSEE, les statistiques individuelles de décès et les systèmes d'information mis en place dans les hôpitaux et dans la branche assurance maladie — mais qui ne relèvent pas stricto sensu du champ de la recherche en épidémiologie — le mode de recueil obligatoire s'applique essentiellement aux déclarations à l'autorité sanitaire de certaines maladies.

La déclaration obligatoire

L'obligation pour les professionnels de santé de déclarer certaines maladies « contagieuses » date d'une loi du 30 novembre 1892.

L'objectif d'origine, qui était d'éviter la propagation de maladies contagieuses, a largement évolué pour s'orienter vers la surveillance épidémiologique. Une rénovation des modes de déclaration a ainsi été amorcée en 1986 tant en ce qui concerne la liste des maladies à déclaration obligatoire (le décret du 10 juin 1986 a ainsi inscrit le sida avéré sur la liste des maladies à déclaration obligatoire) que les modalités de la surveillance.

La loi sur la veille sanitaire du 1er juillet 1998 (article L11 du Code de la santé publique) a consacré cette nouvelle orientation en prévoyant deux modes de surveillance :

— 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 ;
— les maladies qui nécessitent une intervention urgente locale, nationale ou internationale et qui doivent être signalées sans délai, comme par exemple, le choléra, la listériose, la rage ou encore les toxi-infections alimentaires. Elles sont aujourd'hui au nombre de 20.

La lecture du décret 99-363 du 6 mai 1999 permet de constater que la quasi-totalité des maladies énumérées dans la première catégorie sont également visées dans la seconde catégorie, à l'exception, toutefois, du tétanos, de l'hépatite B et de l'infection à VIH. Cette exception est importante, la nature des données susceptibles d'être communiquées à l'autorité sanitaire différant de façon notable selon le mode de signalement. Ainsi, le décret n° 99-362 du 6 mai 1999 prévoit, s'agissant des maladies qui nécessitent une intervention urgente, la possibilité de communiquer, à la demande du médecin inspecteur de la santé publique, l'identité et l'adresse du malade, afin de mettre en place des mesures de prévention et, le cas échéant, de déclencher des investigations pour identifier l'origine de la contamination ou de l'exposition.

Les systèmes de recueil facultatifs des données

Ce mode de recueil est utilisé pour la plupart des études épidémiologiques, qu'il s'agisse des enquêtes de cohorte, qui consistent à suivre sur une période donnée, une population déterminée, des enquêtes dites transversales qui visent à connaître, à un moment précis le phénomène morbide étudié, des enquêtes par sondage auprès d'échantillons de population représentatifs, des enquêtes cas-témoins, pour comparer deux populations distinctes, l'une atteinte d'une pathologie déterminée et l'autre considérée comme saine, des réseaux « sentinelles » qui permettent, à partir d'un réseau de médecins volontaires, de fournir, à intervalles réguliers, des informations sur l'évolution de telle épidémie de grippe ou de bronchiolite.... Selon les cas, les données recueillies sont directement ou indirectement nominatives voire mêmes anonymes.

Les registres de morbidité, qui concernent essentiellement les cancers (il existe aujourd'hui une quarantaine de registres en fonctionnement) permettent, eux, de recenser, dans une zone géographique déterminée, les cas de la pathologie étudiée à partir de données nominatives transmises par les médecins et autres professionnels de santé concernés.

2) LA SURVEILLANCE ÉPIDÉMIOLOGIQUE DU SIDA

Le système actuel de surveillance en France

Le Sida avéré est une maladie à déclaration obligatoire depuis le décret du 10 juin 1986. La CNIL s'est prononcée à plusieurs reprises sur le système d'informatisation des déclarations obligatoires de sida avéré actuellement géré par l'Institut de

Veille Sanitaire (délibération n° 88-91 du 6 septembre 1988, n° 95-101 du 11 juillet 1995, n° 97-025 du 1er avril 1997).

Le circuit des données recueillies et enregistrées à l'IVS est analogue à celui qui existe pour les autres maladies à déclaration obligatoire. C'est au praticien qui diagnostique un cas de sida qu'il appartient d'adresser le formulaire de déclaration obligatoire au médecin inspecteur de la santé de son département sous pli médical confidentiel. Le talon du formulaire qui comporte l'identité exacte du patient est conservé dans le dossier médical du patient. Le médecin inspecteur de la santé du département, après vérification, adresse le formulaire à l'IVS qui saisit alors les données figurant sur le formulaire, à savoir un numéro construit à partir des initiales du nom et du prénom, la date de naissance, le département de domicile ainsi que le sexe, la date de décès, le département de naissance et le pays de domicile, la nationalité et la catégorie socio — professionnelle. Les autres informations collectées et enregistrées sur support informatique sont relatives au diagnostic du Sida et aux caractéristiques des soins. Ces informations sont donc indirectement nominatives et c'est cette caractéristique qui permet de détecter les doublons sur l'ensemble des déclarations effectuées (depuis la mise en œuvre du système, 20 % de doublons ont été ainsi repérés). Après analyse des données, l'IVS retransmet aux médecins inspecteurs des DDASS, les cas de sida répertoriés dans leur département.

Il existe également d'autres systèmes d'information sur le sida, reposant eux, sur un mode de recueil facultatif des informations.

L'INSERM est ainsi chargé, depuis 1987, de suivre une cohorte de volontaires séropositifs (cohorte SEROCO), afin de déterminer les facteurs dits « pronostiques » de la survenue d'un sida, d'évaluer les traitements administrés lors d'essais thérapeutiques et de constituer une « sérothèque » permettant de conserver des échantillons de prélèvements sanguins à des fins de recherche (avis favorable de la CNIL du 17 novembre 1987). Le fichier est directement nominatif. En outre, de nombreuses données « sensibles » sont recueillies qui concernent le statut familial, socio-professionnel, comportemental, clinique et biologique. Le consentement exprès des personnes, contresigné du médecin, est bien évidemment recueilli.

Par ailleurs, en 1987, l'INSERM a été chargé de la coordination des centres d'information et de soins pour l'immunodéficience humaine (CISIH) mis en place dans les établissements de soins prenant en charge des malades atteints du Sida, essentiellement dans les services de maladies infectieuses. L'INSERM a ainsi la tâche de collecter, d'exploiter et d'analyser, de façon cohérente et coordonnée l'ensemble des données épidémiologiques fournies par les centres.

La CNIL s'est prononcée à plusieurs reprises sur les fichiers informatiques mis en œuvre tant dans ces centres qu'à l'INSERM (notamment délibération n° 91-071 du 10 septembre 1991). Les données collectées au niveau des services sont nominatives mais font l'objet, avant leur transmission à l'INSERM d'une anonymisation.

Enfin, des systèmes anonymes de surveillance des découvertes de la séropositivité ont été mis en place entre 1988 et 1996, qu'il s'agisse du réseau national RENAVI de 350 laboratoires d'analyses, destiné à étudier les tendances à long terme et les variations saisonnières de l'activité de dépistage du VIH en France au travers

du suivi anonyme du nombre de tests réalisés par les laboratoires, ou de l'enquête RESORS-VIH menée — dans 13 régions françaises à l'initiative des Observatoires régionaux de la santé (ORS). Le système, abandonné en 1998, associait 71000 médecins et 2100 laboratoires et reposait sur la double participation des laboratoires et des médecins prescripteurs. Le document de collecte des données permettant de signaler la séropositivité, comportait « un volet laboratoire » et un questionnaire médical. Les deux volets étaient renvoyés à l'ORS au moyen d'enveloppes pré-adressées interdisant ainsi toute identification du laboratoire ou du médecin. Dans le souci de garantir l'anonymat des patients et le strict respect du secret professionnel, l'ORS n'avait ainsi connaissance ni du nom du patient, ni de celui du médecin prescripteur, ni de celui du laboratoire.

Les systèmes de surveillance épidémiologiques à l'étranger (sources IVS)

Tous les pays d'Europe de l'Ouest ont mis en place depuis une dizaine d'années des systèmes de déclaration de la séropositivité au VIH, distinctes du sida déclaré, au plan national ou régional.

Ainsi, l'Allemagne dispose depuis 1988 d'un système de déclaration de la séropositivité au VIH qui comporte, s'agissant des éléments d'identification permettant l'élimination des doublons, l'année de naissance, la résidence et un code basé sur le nom. Cette déclaration est, par ailleurs reliée à la déclaration du sida avéré établie distinctement mais qui utilise le même code, ce qui permet de repérer le passage au sida déclaré.

L'Espagne a mis en place très récemment un système de déclaration du VIH comportant les initiales du nom et du prénom ainsi que la date de naissance complète. S'agissant du sida déclaré, le nom complet est collecté.

Au Royaume-Uni, le système national date de 1984 et comporte un code calculé à partir des consonnes du nom complété de la date de naissance. Les informations recueillies sont les mêmes pour le sida avéré.

En Italie, le système est régional et date de 1985. Sont enregistrés, les initiales, la date de naissance et la commune de naissance. Le sida avéré est lui déclaré nominativement.

En Suisse, les initiales du nom et du prénom ont été ajoutées en 1999 aux déclarations de VIH qui ne contenaient auparavant, comme élément d'identification, que la date de naissance et le canton de résidence. Cet ajout permettra également de rapprocher le fichier de celui des déclarations de sida avéré.

Au Danemark, l'adoption d'un identifiant unique (code de sécurité sociale) pour les déclarations de VIH, actuellement en discussion, est présentée comme devant permettre de relier le fichier VIH avec d'autres fichiers de données sanitaires, pour suivre la morbidité, la mortalité et la prise en charge associées à l'infection VIH.

Enfin, aux Etats-Unis, 32 Etats sur 50 ont, comme pour le sida, une surveillance nominative de l'infection à VIH.

Au plan européen, a été crée au milieu des années 1980 un Centre Européen pour la surveillance épidémiologique du sida qui regroupe 48 pays de la région Europe de l'OMS. Chaque trimestre, les pays participant à ce programme européen fournissent au Centre Européen (hébergé en France par l'IVS), des données anonymes sur tous les cas de sida déclarés. Une base de données européenne des cas de sida a ainsi été constituée.

L'évolution des modalités de surveillance épidémiologique du sida

En France, l'évolution de l'épidémie de sida est aujourd'hui mesurée essentiellement grâce aux résultats issus des systèmes d'information précités, et principalement de l'exploitation des déclarations obligatoires de sida avéré. Mais, les statistiques actuellement disponibles à partir des déclarations de sida avéré ne reflètent pas l'évolution actuelle de l'épidémie du sida en France. En effet, les nouvelles modalités de prise en charge des personnes séropositives et en particulier les traitements anti-rétroviraux et les trithérapies permettent de retarder de façon significative voire même de faire régresser l'évolution de la maladie. Dès lors, une baisse relative des cas de sida déclarés ne permet pas pour autant d'en tirer des conclusions quant à l'évolution de l'épidémie. On peut simplement conclure que l'apparition des nouvelles thérapies a eu pour effet de diminuer le nombre de cas de sida avéré sans pour autant en déduire que le nombre de personnes séropositives a diminué.

Aussi, la majorité des interlocuteurs rencontrés par la CNIL s'accorde-t-elle à reconnaître que le système de la seule déclaration du sida au stade de la maladie est insuffisant pour appréhender l'ensemble des aspects de l'épidémie. On estime aujourd'hui, que 5000 cas nouveaux de séropositivité apparaissent par an mais aucun instrument épidémiologique efficace n'existe en France pour mieux cerner les risques et adapter les politiques de prévention.

C'est ce constat qui a conduit à recueillir l'avis des instances scientifiques sur l'opportunité d'inscrire ou non la déclaration de séropositivité dans la liste des maladies à déclaration obligatoire.

Le Conseil National du Sida, (CNS) a émis le 29 janvier 1998 un avis défavorable à l'instauration d'un système de déclaration de nature obligatoire. Tout en reconnaissant les limites de la déclaration du sida avéré, le Conseil National a en effet estimé que le caractère contraignant et obligatoire du signalement de toute séropositivité au VIH comporterait en lui-même des risques d'atteinte aux libertés individuelles importants.

L'Académie Nationale de Médecine s'est, par un avis du 3 mars 1998, prononcée favorablement sur l'opportunité de mettre en place une déclaration à caractère obligatoire de l'infection à VIH « de manière strictement anonyme ». L'Académie de médecine a en effet estimé que la déclaration obligatoire du seul sida avéré, utile et efficace en son temps, est devenue insuffisante, négligeant le nombre beaucoup plus important des sujets infectés et qu'il convenait en conséquence d'élargir la déclaration obligatoire à l'ensemble des contaminés sérologiquement décelés qui conduirait à une meilleure connaissance de l'histoire naturelle de la maladie et de l'efficacité des traitements. L'Académie a enfin considéré que cette déclaration

permettrait, en outre, aux pouvoirs publics d'adapter les actions de prévention, de dépistage et de prise en charge.

L'avis favorable rendu le 29 avril 1998 par le Conseil Supérieur d'Hygiène Publique de France, instance placée auprès du Ministre de la Santé apporte, au-delà des constats d'insuffisance du système de déclaration existant sur le sida, un éclairage sur d'autres points. En premier lieu, s'agissant du circuit de collecte des informations qui devront être recueillies, il indique — et c'est ce que le législateur retiendra dans la loi du 1er juillet 1998 — que le système de recueil des données devrait associer, pour être réellement efficace et exhaustif, tant les laboratoires que les médecins. Il considère, par ailleurs, que le terme de « maladie à déclaration obligatoire » employé jusqu'à présent, notamment par le dernier texte de nature réglementaire ayant mis à jour la liste de ces maladies (décret n° 86-770 du 10 juin 1986), devrait être révisé, « car il peut induire pour certains une confusion avec le terme » dépistage obligatoire « ». Il insiste également sur la nécessité de procéder à une vaste campagne d'information et de sensibilisation, seule à même d'expliquer et de faire accepter le système Enfin, il conclut sur le fait « qu'il sera nécessaire de veiller au respect des règles éthiques et de confidentialité concernant des données indirectement nominatives ».

C'est à la suite de ces avis que le Ministre de la Santé a pris la décision au printemps 1998 d'inscrire la séropositivité parmi la liste des maladies à déclaration obligatoire.

B. De la nécessité de disposer dans le domaine de l'épidémiologie de données directement ou indirectement nominatives

1) LA JUSTIFICATION DU RECOURS À DES DONNÉES NOMINATIVES

En épidémiologie, le recueil des données identifiantes sur les personnes, définies comme des sujets d'observation, et sur les professionnels de santé qui ont fourni l'information, constitue un moyen de discriminer un cas par rapport à un autre, d'éliminer les doubles enregistrements d'autant plus fréquents que les informations sont susceptibles de provenir de sources d'information multiples (ex : médecins hospitaliers, laboratoires...), de rassembler et de vérifier sur un patient déterminé, les renseignements obtenus, de suivre cas par cas l'évolution d'une pathologie ou d'une thérapeutique.

Les justifications du recours à des données identifiantes sont donc nombreuses dans le domaine épidémiologique.

Ainsi, l'élimination des doublons et la vérification des données soit auprès des professionnels de santé qui les ont fournies, soit auprès des patients eux-mêmes, permet de disposer de données fiables et de qualité et de statistiques scientifiquement valables même si des corrections statistiques peuvent parfois être appliquées pour pallier les risques de biais résultant d'informations insuffisantes.

De même le suivi épidémiologique de l'évolution de telle pathologie et de l'impact de telle ou telle thérapeutique peut induire le recueil en continu, sur des cas diagnostiqués, d'informations de suivi, ce qui nécessite alors de procéder à l'appariement des informations autour d'identifiants communs (ex : nom ou initiales du nom et du prénom).

En outre, le chercheur peut avoir le souci de vérifier ou d'approfondir tel ou tel résultat obtenu en procédant, à partir d'une première analyse des données recueillies, à des enquêtes complémentaires qui seront conduites tant auprès des professionnels de santé qu'auprès des patients. Tel est en particulier le cas pour certains registres de morbidité. La conservation, dans le fichier, de données identifiantes peut alors se justifier.

Enfin, une étude épidémiologique peut éventuellement s'accompagner ou être suivie d'actions de prévention ou de dépistage auprès de la population.

2) ETAT DES RECUEILS D'INFORMATIONS EXISTANTS : LES PRATIQUES CONSTATÉES

Selon le type d'études réalisées, la méthodologie employée, le recours ou non à l'outil informatique, les informations recueillies sont donc « plus ou moins nominatives ».

Les systèmes de recueil de données épidémiologiques à caractère obligatoire font généralement appel à des données qui sont indirectement nominatives.

L'étude de certaines filières de soins ou de certaines maladies contagieuses pourra nécessiter le recueil de la localisation géographique précise (commune de résidence) des patients et du service d'hospitalisation ou du médecin concerné. De telles données corrélées avec l'âge des patients peuvent permettre l'identification des personnes concernées, surtout si l'effectif de population est restreint ou si la source d'information est identifiée.

D'autres recherches épidémiologiques feront appel directement à l'identité de la personnes afin d'assurer un recensement aussi exact que possible des cas de la pathologie étudiée et permettre la réalisation d'études complémentaires : tel est le cas, notamment, des registres de cancer.

Il demeure, qu'au delà des justifications précédemment invoquées, le recueil de l'identité complète de la personne peut constituer quelquefois une « facilité » qui rend plus aisée, pour les médecins qui fournissent les informations, la recherche dans les dossiers médicaux, des cas susceptibles d'entrer dans le champ de l'étude. Or, dans bien des cas l'identité complète n'est pas nécessaire et pourrait être remplacée par les initiales du nom ou par un numéro d'ordre.

La CNIL a toujours favorisé la mise en place et le développement de mesures de sécurité spécifiques de nature à garantir la confidentialité des données : cryptage, séparation des données relatives à l'identité des personnes, des renseignements proprement médicaux, « appauvrissement » des données (par exemple en

recueillant l'âge de la personne plutôt que sa date de naissance), élaboration de systèmes plus complexes « d'anonymisation » à la source des données d'identification.

Ainsi, l'INSERM a mis en place en 1988, avec l'accord de la CNIL un système d'information épidémiologique sur le sida faisant appel à un système d'anonymisation à la source — c'est-à-dire dans les services de maladies infectieuses hospitaliers — des données d'identification des patients atteints du sida. Ce dispositif, soumis à l'époque à l'expertise du Service central de sécurité des systèmes d'information (SCSSI) et dit « algorithme de San Marco », du nom du responsable du laboratoire de santé publique de Marseille qui a développé ce système, permet, grâce à un algorithme particulier, de coder de façon irréversible les nom, prénom et date de naissance du patient, c'est-à-dire de produire un numéro non signifiant et non identifiant à partir de ces trois informations. Toute transmission ultérieure d'informations accompagnées du numéro codé, spécifique à une personne, peut permettre de savoir qu'il s'agit du même patient sans qu'il soit possible de l'identifier ni directement ni indirectement.

En 1996, dans le cadre de la mise en place du programme de médicalisation des systèmes d'information (PMSI) dans les établissements de santé privés, la CNIL s'est également prononcée sur un dispositif d'anonymisation qui limite les risques d'identification tout en permettant d'assurer un lien (« chaînage ») entre les différents séjours d'un patient au sein de l'établissement. Cette technique fait appel à un algorithme dit de « hachage » (SHA) qui permet de transformer de façon non réversible les données nominatives en un numéro anonyme et unique permettant, sans qu'il soit possible d'identifier le patient, d'apparier cependant sur un même individu les données relatives à ses séjours successifs dans l'établissement. Ce dispositif est développé par le Centre d'Etudes des Sécurités du Système d'Information (CESSI) qui dépend de la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés et a également été expertisé par le SCSSI.

Ces dispositifs, qui sont en réalité de petits programmes informatiques, supposent cependant que les professionnels et établissements de santé qui procèdent à la source à la collecte des données disposent de moyens informatiques.

C. Les recommandations de la CNIL

Quelques constats et rappels s'imposent.

Sur le principe même de la déclaration obligatoire

Il convient de relever que les différentes associations consultées par la CNIL sont dans leur grande majorité favorables au caractère obligatoire de la déclaration de séropositivité, quelques unes d'entre elles exprimant cependant le souhait que l'établissement de la déclaration soit soumis au consentement de la personne. La déclaration obligatoire implique cependant non seulement l'obligation pour les médecins et les laboratoires de signaler les cas diagnostiqués mais également l'impossibilité pour le patient de s'opposer à cette collecte d'informations. Dès lors, le dispositif est, dans son principe même, incompatible avec le recueil du consente-

ment préalable de la personne concernée avant toute collecte d'informations sur sa séropositivité. En un mot, on ne peut tout à la fois se déclarer favorable à la déclaration obligatoire de séropositivité et favorable au principe du consentement de la personne.

Mais, l'impossibilité pour les personnes de pouvoir exercer un droit d'opposition rend d'autant plus impérieuse la nécessité d'une information claire et complète des personnes concernées sur le système mis en place, la mise en œuvre de garanties de confidentialité, l'appréciation rigoureuse, au regard des nécessités de santé publique, de la pertinence des informations collectées et de manière plus spécifique le sort à réserver aux résultats de tests de séropositivité pratiqués par les centres de dépistage anonymes et gratuits.

Sur la nécessaire dimension européenne du système de surveillance épidémiologique

Un système européen de surveillance épidémiologique du sida a été mis en place, ce qui nécessite à l'évidence que le centre européen chargé du système qui est, d'ailleurs, géré par la France dispose, de la part de l'ensemble des pays participant au système, d'informations répondant à des définitions et critères communs. Or actuellement, si la France est en mesure de communiquer au centre européen des données sur les cas de sida avéré, il n'en est pas de même pour la séropositivité au VIH. Les données actuellement traitées par le centre européen sont les suivantes : numéro séquentiel propre à chaque pays, pays, sexe, âge, date du diagnostic, département, statut vital, modes de contamination et caractéristiques de la pathologie.

Sur les fichiers de personnes séropositives

Des fichiers directement nominatifs comportant des informations relatives à des personnes séropositives existent, qu'il s'agisse des dossiers médicaux tenus dans les services hospitaliers, les cabinets médicaux ou les laboratoires d'analyses, des fichiers de gestion de remboursement détenus par les organismes de sécurité sociale (aujourd'hui, toute personne découverte séropositive au VIH et qui suit un traitement médical est prise en charge à 100 %) ou encore des fichiers constitués par les associations d'aide aux personnes atteintes par le VIH. Ces fichiers, qui nécessitent, bien entendu, des mesures de protection particulières, ne sont pas cependant spécifiques aux personnes séropositives au VIH.

Le système de surveillance épidémiologique des cas de séropositivité tel qu'il est envisagé suppose, lui, la constitution d'un fichier spécifique aux personnes séropositives. C'est cette spécificité, cette « spécialité » qui fait naturellement de ce fichier un fichier très « sensible ».

Il convient cependant de souligner que les traitements d'informations doivent être gérés sous la responsabilité d'un établissement public spécifiquement chargé de cette surveillance, par des médecins et chercheurs dûment habilités et astreints au secret professionnel. Il est à cet égard important de noter qu'aucune dérive ayant entraîné une rupture de la confidentialité n'a été constatée depuis la mise en place en 1988 de la déclaration obligatoire du sida avéré. Les associations de malades le

confirment : les risques de rupture de la confidentialité et de discrimination sociale ou professionnelle en raison de l'état de santé ont pu être constatés dans les relations employeur/employé ou dans le domaine des assurances ou de la banque, aucune ne l'a été à partir d'un « mésusage » des données traitées par l'IVS.

LES RECOMMANDATIONS

Une nécessaire clarification des objectifs de la surveillance épidémiologique

Si le principe de la déclaration obligatoire ne paraît pas contesté, il apparaît toutefois nécessaire que les pouvoirs publics clarifient les objectifs de ce recueil d'informations.

En effet, s'agit-il seulement d'obtenir, année par année, un état exhaustif du nombre de personnes séropositives en France permettant de connaître les tendances et l'évolution de l'épidémie de sida et d'évaluer, de façon globale, l'impact des actions de prévention ? Ou bien l'objectif est-il également d'instituer une véritable surveillance épidémiologique de l'évolution des cas d'infection par le VIH, du stade de la découverte de la séropositivité à l'apparition éventuelle du sida avéré ? Cette dernière hypothèse dans laquelle il deviendrait possible de mesurer, de façon fine, l'impact des actions thérapeutiques et de prévention nécessiterait alors un suivi des cas et en particulier un rapprochement avec le système des déclarations obligatoires des cas de sida.

Ce choix d'objectifs qu'il appartient aux pouvoirs publics de définir clairement au regard des impératifs de santé publique emporte des conséquences importantes tant sur la nature des données susceptibles d'être collectées que sur leur durée de conservation et les liens éventuels avec d'autres systèmes de surveillance. Il implique en conséquence des choix en termes de protection des données.

Si, en effet, il s'agit d'assurer un dénombrement annuel des cas de séropositivité pour disposer d'une « photographie » de l'infection en France, il n'est nul besoin de traiter d'informations qui puissent peu ou prou présenter un caractère nominatif. Il ne paraît pas non plus nécessaire de conserver sur une longue période ces données.

Si, en revanche, la finalité du système des déclarations obligatoires, telle qu'elle semble se dessiner actuellement, est d'assurer un suivi épidémiologique des cas de séropositivité au virus du VIH et de mesurer l'évolution de l'épidémie de sida en France, elle ne peut être réalisée que par la collecte de données qui doivent être, à la source, individualisées, afin de permettre de détecter les doublons, de vérifier les données auprès des professionnels de santé et, le cas échéant, d'apparier les données avec celles collectées dans le cadre du sida avéré.

Un tel choix nécessiterait de disposer de données suffisamment discriminantes, de telle sorte qu'on puisse distinguer un cas d'un autre, de conserver les informations pendant une durée plus longue.

Sur ce point, l'Institut de Veille Sanitaire, à partir des déclarations obligatoires de sida avéré dont il dispose, a tenté d'analyser l'impact d'un « appauvrissement » des informations indirectement nominatives figurant sur les déclarations de sida, à savoir actuellement : les initiales du nom et du prénom, la date de naissance complète et le département de domicile.

Actuellement, le traitement de ces informations indirectement nominatives permet de repérer dans une proportion de plus de 99 % les cas de doublons supposés. En revanche, la suppression des initiales conduirait à enregistrer dans la base 20 % des doublons correspondant en fait à une seule et même personne. Ce pourcentage atteindrait plus de 75 % si les initiales et le jour de naissance étaient supprimés.

Un « appauvrissement » trop important des données peut donc fausser de façon conséquente les statistiques et remettre en cause la fiabilité scientifique de la surveillance épidémiologique.

Par ailleurs, compte tenu notamment de l'allongement du délai aujourd'hui constaté entre la découverte d'une séropositivité et la déclaration d'un sida, les données devraient nécessairement être conservées longtemps, même si les positions exprimées par les associations sont divergentes. Il convient de noter que la durée de conservation par l'IVS des données indirectement nominatives collectées dans le cadre du système de la déclaration obligatoire de sida avéré est, aujourd'hui, de 10 ans.

Par ailleurs, le lien qui serait effectué, le cas échéant, avec les données contenues dans le fichier du sida déclaré, afin notamment d'évaluer le temps qui s'écoule entre la découverte d'une séropositivité et un éventuel passage au stade du sida ou encore de connaître le statut vital de la personne, nécessiterait d'adopter pour la séropositivité le même système d'identification que pour le sida.

Scientifiquement, le recueil à la source des initiales du nom et du prénom ainsi que de la date de naissance, qui pourraient certes être transmis sous une forme codée, paraît dès lors indispensable. En outre, la mention sur la déclaration des coordonnées des médecins déclarants qui confère, certes, un certain caractère nominatif à la déclaration, se justifie par la nécessité de pouvoir, le cas échéant, vérifier les informations fournies et assurer ainsi des statistiques de qualité. Selon l'IVS un tiers des déclarations de sida qui lui parviennent nécessite un retour auprès des médecins déclarants pour compléter les données manquantes ou vérifier telle ou telle information.

Le renforcement des mesures de confidentialité :
vers l'adoption d'un système dit « d'anonymisation » à la source :

Eu égard à la sensibilité des informations traitées, toutes garanties doivent être prises pour assurer la confidentialité des informations et protéger l'anonymat des personnes, ainsi que le prescrit la loi sur la veille sanitaire.

Le recours à des techniques dites « d'anonymisation » à la source est de nature à répondre aux besoins particuliers de confidentialité que nécessite la mise en place d'un tel système en évitant que ne soient conservées tant au plan local que

national des données qui, par recoupement, pourraient permettre l'identification des personnes.

Mais si les pouvoirs publics s'orientent effectivement vers une telle solution, encore conviendra — t-il de déterminer celles des informations qui seront utilisées par l'algorithme utilisé pour produire le numéro, et d'évaluer les conséquences de la mise en place d'un tel dispositif.

La procédure de codage des données d'identification pourrait être effectuée à la source par les biologistes qui transmettraient aux médecins prescripteurs, avec le résultat du test pratiqué, le formulaire épidémiologique comportant pour toute référence le code produit par l'algorithme à charge pour les médecins de compléter les variables épidémiologiques de la notification. Un tel dispositif pourrait être de nature à lever, au moins en partie, les réserves exprimées par certaines associations auditionnées par la CNIL sur la participation au dispositif des laboratoires.

Mais au-delà de l'anonymisation à la source, des mesures de protection devraient être adoptées pour, à la fois, sécuriser les fichiers informatiques (notamment par un cryptage) et trancher le sort des déclarations papier en particulier au niveau des DDASS. La transmission aux médecins inspecteurs des DDASS des déclarations devrait ainsi d'effectuer, dans tous les cas, dans des conditions garantissant la confidentialité, telles que par exemple l'envoi sous pli confidentiel des déclarations au médecin chargé de la surveillance épidémiologique du sida.En outre, une fois le travail de validation effectué par les médecins au niveau départemental et les données transmises à l'IVS, aucune déclaration ne devrait être conservée.

Une attention particulière doit, enfin, être portée à la diffusion des statistiques établies à partir des données collectées et traitées afin d'éviter tout risque d'identification des personnes. En effet, toutes précautions doivent être prises pour que la diffusion de statistiques sur l'état de la séropositivité en France n'aboutisse pas à publier des données qui, corrélées avec d'autres, pourraient permettre d'identifier un individu.

La nature sensible des autres informations :

La mise en place d'une « anonymisation » à la source et de mesures de sécurité adéquates ne dispense pas de s'interroger sur la pertinence des autres informations appelées à figurer sur la déclaration de séropositivité.

Il s'agit, en particulier, du code postal de résidence, de la profession et de l'origine géographique.

— Le code postal de domicile

Cette variable qu'il était prévu de mentionner sur la déclaration de séropositivité était présentée comme ayant pour objet de permettre aux médecins inspecteurs des DDASS de mieux cibler les actions de prévention locale en fonction, notamment, de l'importance relative du nombre de personnes séropositives. Par exemple, la connaissance, dans une zone géographique donnée, d'un nombre relativement important de toxicomanes séropositifs pourrait conduire les autorités sanitaires à décider de l'implantation dans cette zone de distributeurs de seringues stériles.

Mais force est de constater que la pertinence du recueil de cette donnée, notamment au plan national, n'est pas à ce jour réellement démontrée. En outre, sa collecte et son exploitation pourraient être de nature à permettre une localisation géographique précise des cas de séropositivité, surtout dans les communes de moyenne importance avec tous les risques de rupture de la confidentialité et de stigmatisation qui pourraient en résulter.

Dès lors le recueil sous une forme aussi détaillée que le code postal de domicile, du lieu de résidence des personnes séropositives peut paraître excessif au regard des objectifs recherchés.

— La profession

Cette variable peut présenter un intérêt dans la mesure où elle constitue une indication de la situation sociale des personnes séropositives. S'il peut effectivement être utile sur le plan épidémiologique de mieux connaître les catégories de situation socio-professionnelles des personnes et en particulier la proportion de chômeurs, d'étudiants, ou de cadres.... afin de mieux cibler les actions de prévention, il ne paraît pas nécessaire de disposer du détail de la profession précise des personnes concernées. Dès lors, seule la mention des catégories socio-professionnelles selon la nomenclature de l'INSEE ou d'une nomenclature inspirée de celle-ci paraît pertinente.

L'adoption d'une liste simplifiée des catégories socio-professionnelles — la nomenclature de l'INSEE comportant plus de trente catégories — aurait le mérite de simplifier la tâche du médecin chargé de compléter le formulaire, l'assimilation d'une profession à une catégorie socio-professionnelle donnée n'allant pas toujours de soi.

— L'origine géographique

Le formulaire de déclaration prévoyait la collecte d'une information sur l'origine géographique de la personne séropositive et du partenaire sexuel en distinguant l'Afrique Sub-Saharienne, les Caraïbes et les autres pays. Cette formulation pourrait donner à penser que c'est l'origine raciale des personnes ou de leurs partenaires qui est recherchée.

Tel n'est pas en réalité l'objet du recueil de cette donnée. Il s'agit de déterminer sur le plan épidémiologique si les personnes ont vécu ou séjourné dans des pays qui connaissent une forte épidémie de sida et où la transmission hétérosexuelle du virus est actuellement prédominante. Il convient d'ajouter qu'une rubrique de même nature figure parmi les données transmises au centre européen pour la surveillance épidémiologique du sida, sans qu'il soit pour autant fait référence à telle ou telle zone géographique du monde. Il est demandé, en effet, si la personne est originaire d'un pays où la transmission hétérosexuelle est prédominante ou a eu des relations sexuelles avec une personne originaire ou ayant vécu dans un pays où la contamination hétérosexuelle est prédominante. La même rubrique figure d'ailleurs sur les déclarations obligatoires de sida avéré.

Les différentes associations auditionnées par la CNIL ont, dans leur majorité, exprimé leur opposition à la collecte de l'information telle qu'elle figure actuellement sur les déclarations.

Si la Commission ne conteste pas l'utilité épidémiologique d'une telle information, il lui apparaît toutefois nécessaire de lever toute ambiguïté sur sa signification en explicitant les objectifs recherchés ou en recommandant une formulation plus explicite.

La nécessité d'exclure du dispositif de surveillance les centres de dépistage anonymes et gratuits

L'activité des centres de dépistage anonymes et gratuits a connu depuis leur mise en place en 1987 une progression constante. Aujourd'hui, une personne sur cinq se fait dépister dans un CDAG. Dans ce cas, les personnes n'ont à révéler ni leur nom, ni leur adresse. Toute personne qui souhaite bénéficier d'un dépistage anonyme dans ces centres se voit attribuer, lors de sa venue, un numéro séquentiel reporté sur une fiche, qu'elle devra présenter à nouveau lors de la remise des résultats de sa sérologie.

L'instauration d'une déclaration obligatoire fondée sur une identification même indirecte de la personne, et fût-elle codée, est, par définition, contraire au principe de l'anonymat des centres de dépistage anonymes et gratuits.

Inclure les CDAG dans le dispositif de la déclaration obligatoire de séropositivité, serait d'une part, prendre le risque de briser la relation de confiance instaurée entre le professionnel de santé et le patient, d'autre part remettre en cause le droit pour la personne de choisir le lieu et les conditions de son dépistage, peut-être et surtout, le dissuader de se faire dépister. Il convient de noter, en outre, que dans les pays qui disposent de tels centres, le dispositif des déclarations obligatoires ne s'y applique pas.

L'exclusion des CDAG du dispositif ne devrait pas nuire à la recherche épidémiologique. En effet, les personnes qui se révélerent séropositives, à l'issue d'un test pratiqué dans un CDAG, sont dans le cadre des relations de confiance qu'elles entretiennent avec le médecin, orientées vers des services de soins.

C'est à ce stade, et à ce stade seulement, dans une deuxième étape, que la séropositivité de la personne concernée pourra être déclarée. Elle ne doit pas l'être dans les CDAG.

La nécessité d'assurer une plus grande transparence dans la mise en place du dispositif

La réflexion entreprise par la CNIL démontre l'utilité d'une concertation avec tous les acteurs du dispositif. En effet, la légitime sensibilité manifestée par l'opinion publique à l'égard de la mise en place de fichiers dans le domaine du sida rend indispensable la plus grande transparence tant à l'égard des patients.

Le caractère obligatoire de la déclaration de l'infection par le virus de l'immunodéficience humaine, quel que soit le stade de la maladie doit être accompagné d'une information très claire de la personne sur les objectifs et les modalités du dispositif de sorte que chacun puisse être pleinement convaincu à la fois de

l'importance majeure que revêt, en termes de santé publique, la lutte contre l'épidémie de sida.

II. LA DIFFUSION DES DONNÉES SOUS CONDITIONS

A. Le chapitre V ter de la loi du 6 janvier 1978 : l'encadrement des traitements de données médicales à des fins d'évaluation

Depuis la loi du 31 décembre 1991 portant réforme hospitalière (articles L710-6 et L710-7 du code de la santé publique), les établissements de santé, dans le cadre de ce que l'on appelle le 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 —, sont tenus de fournir régulièrement à leur tutelle, et en particulier au ministère de la Santé, un certain nombre d'indicateurs sur leurs activités de soins, parmi lesquels des données individualisées par patient, les Résumés de Sortie Anonymes (RSA), qui indiquent, en particulier, pour chaque séjour, l'âge du patient, la durée de séjour, la pathologie diagnostiquée, les actes pratiqués, l'établissement où il a été hospitalisé. L'identité des patients n'est jamais révélée.

La même obligation est faite aux cliniques privées, tenues d'adresser à la CNAMTS et à l'Etat des résumés de sortie et des informations financières permettant ainsi l'élaboration d'une classification des prestations d'hospitalisation tenant compte des traitements par pathologie.

La CNIL a eu l'occasion de délibérer à de nombreuses reprises sur les modalités de mise en place du PMSI dans les établissements de santé tant publics que privés.

Au sein de chaque établissement de santé, les médecins responsables des départements d'information médicale ont pour mission de recueillir et de traiter les informations médicales qu'ils reçoivent de chaque service et de les retransmettre, sous la forme de résumés de sortie anonymes (RSA), à la direction de l'établissement ainsi qu'aux Agences régionales d'hospitalisation, aux directions régionales des affaires sanitaires et sociales, aux Caisses régionales d'assurance maladie, et au ministère de la Santé. Celui-ci les fait traiter par un de ses services, le centre de traitement de l'information du PMSI (CTIP).

Les RSA ont longtemps été jugés anonymes, comme ne permettant aucunement, ni directement, ni indirectement d'identifier les personnes, et donc considérés par la CADA comme des documents administratifs communicables. Ils pouvaient donc être transmis à tout tiers en faisant la demande : organismes de recherche, sociétés savantes, organes de presse.... A partir des informations ainsi transmises, « un palmarès » et un guide des hôpitaux ont ainsi été publiés en 1998 et en 1999.

Or, il s'est avéré à la suite de travaux statistiques menés en 1998 par la direction des hôpitaux, que ces « RSA » n'étaient pas si anonymes que cela et que l'exploitation des résumés permettait, dans un nombre considérable de cas, de connaître, par recoupement, le motif d'hospitalisation de personnes par ailleurs identifiées.

1) LA POSITION DE LA CNIL

Saisie par la direction des hôpitaux de cette difficulté, la CNIL a tout d'abord constaté que les données figurant sur les RSA étaient certes moins anonymes qu'on le croyait mais beaucoup moins identifiantes que certains le disent. En effet, un résumé de sortie pris isolément ne permet pas à lui seul d'identifier une personne. Ce n'est que si l'on sait que Monsieur X a été hospitalisé ou est décédé à l'hôpital Y que l'exploitation des résumés de sortie sur cet hôpital permet sans difficulté de déterminer pour quel motif cette personne a été hospitalisée ou est décédée.

Dès lors, la Commission, tout en soulignant la nécessité d'un nouvel encadrement juridique, a tenu à rappeler que la protection des données à caractère personnel ne devait pas faire obstacle au droit à l'information et a donc considéré que, dans un esprit de transparence administrative, il importait de rechercher des solutions qui, tout en préservant la confidentialité des données, permettent de répondre aux besoins d'information exprimés, soit par la diffusion de statistiques soit par la diffusion de données individuelles dans des conditions à définir avec la CNIL.

Le Ministre de l'Emploi et de la Solidarité a estimé qu'un nouvel encadrement législatif devait intervenir au plus tôt.

C'est dans ces conditions qu'un article spécifique a été introduit dans le projet de loi relatif à la couverture maladie universelle.

La CNIL, saisie du projet de loi, a rendu le 18 février 1999 un avis défavorable sur le texte qui lui était présenté en particulier au motif que la procédure d'autorisation alors prévue — demande d'avis auprès d'un comité ad hoc et demande d'autorisation auprès de la CNIL — était, compte tenu du caractère très indirectement nominatif des données concernées, excessive et inopportune.

Le projet de loi finalement soumis au Parlement a confié cependant à la CNIL la mission d'autoriser la communication des données.

Cette disposition, qualifiée, au cours des débats parlementaires « d'article liberticide, d'atteinte à la liberté de la presse et au droit à l'information de tous les français sur le système de soins », a suscité d'assez vives controverses et, comme d'autres dispositions de la loi CMU a fait l'objet d'un recours devant le Conseil Constitutionnel au motif que cet article porterait atteinte à la liberté de communication énoncée à l'article 11 de la Déclaration des droits de l'homme et du citoyen et que les formalités prévues auprès de la CNIL, ne constituaient pas, selon les requérants, « une garantie suffisante pour éviter la rupture de l'anonymat ».

Le Conseil, après avoir rappelé qu'il résultait des termes mêmes de la loi, que les données de santé, si elles n'étaient ni directement ni indirectement

nominatives, pouvaient être librement communiquées, a considéré qu'en subordonnant la communication des données de santé susceptibles de permettre l'identification des personnes à l'autorisation de la CNIL, le législateur avait, sans méconnaître l'article 11 de la Déclaration des droits de l'homme et du citoyen, fixé en l'espèce des modalités assurant le respect de la vie privée.

Cette disposition (article 41 de la loi du 27 juillet 1999 portant création d'une couverture maladie universelle) a en conséquence été déclarée conforme à la Constitution.

2) LES NOUVELLES DISPOSITIONS DE LA LOI DU 6 JANVIER 1978

La loi informatique et libertés comporte désormais un chapitre V ter consacré « aux traitements de données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention » ; cinq nouvelles dispositions (articles 40-11 à 40-15) ont ainsi été ajoutées à la loi.

Le dispositif législatif adopté — plus large que le champ d'application initialement envisagé — a pour objet de préciser les conditions dans lesquelles des données de santé, qu'elles soient issues des professionnels de santé eux-même, des systèmes d'information hospitaliers, ou des fichiers des caisses de sécurité sociale, peuvent être diffusées et exploitées à des fins d'évaluation des pratiques de soins et de prévention.

Tout en rappelant le principe d'anonymat qui doit présider à la transmission des données tant aux autorités sanitaires qu'aux tiers, l'article 40-12 prévoit cependant des dérogations à ce principe et la possibilité de transmettre des données indirectement nominatives sous réserve notamment qu'elles ne comportent ni le nom, ni le prénom du patient, ni son numéro de sécurité sociale et que la communication des données soit autorisée par la CNIL.

Une procédure spécifique d'autorisation a donc été instituée pour les traitements de données personnelles de santé réalisés à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention.

L'article 40-13 de la loi précise l'étendue du contrôle de la CNIL et prévoit ainsi que pour chaque demande, la CNIL vérifie « 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 », « s'assure 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 ».

Il appartient 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.

A l'égal de la procédure d'autorisation prévue pour les fichiers de recherche médicale, la loi n'opère aucune distinction entre secteur public et secteur privé.

L'article 40-14 prévoit que la commission dispose d'un délai de deux mois, renouvelable une fois, pour se prononcer. A défaut de réponse dans ce délai, ce silence vaut décision de rejet et non accord tacite, comme c'est le cas pour les demandes d'avis et les demandes d'autorisation pour les fichiers de recherche, présentées respectivement en application des articles 15 et 40-2 de la loi.

Enfin, dans le souci d'alléger les procédures, l'article 10 de la loi du 6 janvier 1978 a été complété de façon à permettre à la Commission de déléguer au président de la CNIL ses attributions en ce qui concerne l'examen des demandes et la délivrance des autorisations.

Un décret du 27 octobre 1999 a précisé les modalités d'instruction, par la Commission, des demandes d'autorisation.

B. Les soins passés en revue

La revue Sciences et Avenir et le Figaro magazine ont été les premiers à saisir la CNIL de demandes d'autorisation pour obtenir communication des résumés de sortie anonymes issus des bases nationales constituées en 1997 et en 1998 par la direction des Hôpitaux et par la CNAMTS à partir des informations fournies par les établissements de santé publics et privés dans le cadre du Programme de Médicalisation des Systèmes d'Information (PMSI).

Dans un cas comme dans l'autre, il s'agit de réaliser une analyse de l'activité hospitalière tant publique que privée, ceci dans la perspective de publier en particulier un classement, établissement par établissement, des hôpitaux et des cliniques, selon un certain nombre de critères.

L'objectif est très clairement d'informer le public sur l'activité hospitalière en France, sous la forme d'un palmarès des hôpitaux, à l'égal de ce qui se fait déjà depuis plusieurs années aux Etats-Unis.

En premier lieu, la CNIL a demandé que les deux revues s'engagent, par écrit, à respecter et à faire respecter, en particulier par la société sous traitante, les règles suivantes :
— n'utiliser les fichiers transmis qu'à des fins d'analyse comparative de l'activité hospitalière ;
— respecter et 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 ;
— 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 ;
— ne pas rétrocéder ou divulguer à tout tiers les informations fournies sous quelque forme que ce soit ;
— 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 ;

— ne pas utiliser de façon détournée les informations transmises, notamment à des fins de recherche ou d'identification des personnes ;
— diffuser les résultats uniquement sous forme de statistiques agrégées de telle sorte que les personnes ne puissent être identifiées ;
— à la fin de la durée autorisée de conservation des RSA, procéder à la destruction de tous les fichiers informatisés stockant les informations de base et les informations traitées ainsi que les supports des informations.

En deuxième lieu, la CNIL s'est attachée à concilier l'intérêt des études et publications projetées et la vie privée des patients dont il convenait d'éviter toute réidentification possible.

A ce titre, la communication de l'information relative au mois de sortie du patient n'a pas été autorisée. En pratique, cette information n'est pas utile pour déterminer la durée du séjour qui figure, en tant que telle, dans le RSA. En revanche le mois de sortie est de nature à permettre une identification indirecte des personnes concernées.

S'agissant des informations administratives sur le patient, la Commission a estimé que l'indication précise de l'âge devait être remplacée par la notion de tranches d'âge de 5 ans en 5 ans. De même, la CNIL a autorisé la communication de l'information relative au département de résidence des patients mais non le code postal de la commune.

S'agissant enfin de la communication de l'indication du décès du patient, la Commission, tout en considérant que l'analyse de la mortalité hospitalière était un objectif d'étude parfaitement légitime, a toutefois estimé que la transmission systématique de l'indication relative aux décès n'apparaissait pas, en l'état, pertinente dans la mesure où, selon les indications fournies par la direction des hôpitaux, cette rubrique n'étant systématiquement remplie que pour certaines pathologies spécifiques, la fiabilité des études de mortalité projetées ne saurait reposer sur un champ informationnel insuffisamment renseigné. En revanche, la Commission a considéré que les journaux devaient avoir communication de cette information lorsque pour certaines pathologies déterminées, l'indication du décès figure dans la classification des groupes homogènes de malades, sous des codes spécifiques.

Au début de l'année 2000, la CNIL, suivant la méthodologie d'instruction adoptée pour les deux premières demandes, a autorisé trois études présentées respectivement par la Fédération des établissements hospitaliers et d'assistance privés à but non lucratif (FEHAP) qui souhaitait obtenir à des fins d'évaluation de l'activité hospitalière des données issues du PMSI, par l'Agence régionale de l'hospitalisation d'Ile de France, qui envisageait de recueillir des données auprès des services d'urgence à des fins d'analyse de la stratégie thérapeutique dans l'infarctus du myocarde et enfin, par le Comité médical paritaire local des médecins généralistes de Paris, organisme paritaire associant l'assurance maladie et les syndicats médicaux qui, dans le cadre d'une étude portant sur l'évaluation collective des prescriptions médicales dans la rhinopharyngite de l'enfant, souhaitait recueillir des données auprès de médecins généralistes. (délibérations n° 00-001, 00-002 et 00-00 3 du 13 janvier 2000).

Délibération n° 99-061 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Sciences et avenir » 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 nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 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 nº 78774 du 17 juillet 1978 modifié et notamment son chapitre IV ;

Vu la demande d'autorisation présentée par la revue « Sciences et Avenir » ;

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 revue « Sciences et Avenir » 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 détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1997 et en 1998 par les établissements de santé publics ou privés, y compris l'Assistance Publique des Hôpitaux de Paris et les Hospices Civils de Lyon ;

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) 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 actes pratiqués ; qu'ainsi, l'identité des patients n'est en aucun cas communiquée ;

Considérant que l'article 40-13 de la loi du 6 janvier 1978, issu de l'article 41 de la loi du 27 juillet 1998, 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 systè-

mes 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 revue sollicite l'obtention du contenu intégral des « résumés de sortie anonymes », pour réaliser une analyse de l'activité hospitalière tant publique que privée, dans la perspective de publier en particulier un classement, établissement par établissement, des hôpitaux et des cliniques, selon un certain nombre de critères ; qu'il serait en particulier procédé à une étude qualitative des principaux services médicaux (cardiologie, orthopédie, urologie, gynécologie, etc.) et à des études portant sur les durées moyennes de séjour par pathologie, sur des pathologies et actes médicaux spécifiques, sur la mortalité par pathologie, par établissement et par service ; que les analyses produites feraient l'objet d'une validation auprès de la conférence des directeurs d'hôpitaux ;

Considérant qu'il y a lieu de rappeler, d'une part, que les « résumés de sortie 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 » 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 l'information des citoyens sur l'état du système de santé en France et en particulier sur l'activité hospitalière 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 revue prévoit que l'ensemble des traitements informatiques soit réalisé, sous la responsabilité du directeur de la rédaction, au siège de la revue, sur trois ordinateurs fonctionnant en réseau fermé, accessi-

bles uniquement à l'équipe chargée des travaux de recherche, soit cinq personnes (dont un médecin) ; 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 directeur de la rédaction s'engage ainsi que ces collaborateurs :
— à n'utiliser les fichiers qu'à des fins d'analyse comparative de l'activité hospitalière ;
— 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 directeur de la rédaction de Sciences et Avenir 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 ; qu'il importe que les résultats publiés ne soient diffusés que sous forme de pourcentages ;

Considérant que la revue envisage de conserver les données qui lui seraient transmises pendant une durée de 3 ans qu'elle justifie, d'une part, par le souci de pouvoir se défendre en justice en cas de contentieux et, d'autre part, pour pouvoir entreprendre des études sur une période plus longue ;

Considérant, toutefois, 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 pour publication des résultats, soit une durée de 10 mois ; qu'un délai supplémentaire après publication doit également être prévu pour d'éventuels traitements supplémentaires ;

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 que la communication de l'indication du mois de sortie, n'est pas pertinente dans la mesure où l'information sur la durée de séjour figure, en tant que telle, dans le « résumé de séjour anonyme » et sera communiquée au demandeur ; qu'au surplus elle est de nature à permettre une identification indirecte des personnes concernées ;

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 l'analyse de la notoriété des établissements de santé ne justifie pas que soient transmis l'intégralité des codes géographiques du lieu de résidence des patients, l'indication du département de résidence étant un des éléments suffisant pour mesurer l'attractivité d'un établissement ;

Considérant que la transmission systématique de l'indication relative aux décès n'apparaît pas, en l'état, pertinente dans la mesure où n'étant systématiquement remplie que pour certaines pathologies spécifiques, la fiabilité des études de mortalité projetées ne saurait reposer sur un champ informationnel n'étant pas systématiquement renseignée ; qu'en revanche lorsque, pour certaines pathologies déterminées, l'indication du décès figure dans la classification des groupes homogènes de malades, sous des codes spécifiques, la revue pourra en avoir communication ;

Considérant en conséquence que la communication par la direction des hôpitaux et par la CNAMTS des résumés de sortie anonymes devra être expurgée de l'indication, dans la rubrique « mode de sortie », du décès ;

Autorise la revue « Science et Avenir » à obtenir 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 détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1997 et en 1998 par les établissements de santé publics ou privés, y compris l'Assistance Publique des Hôpitaux de Paris et les Hospices Civils de Lyon, sous réserves que :
— l'indication du mois de sortie ne soit pas communiquée ;
— 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 ;
— le code géographique de résidence soit remplacé par la seule indication du département de résidence du patient — l'indication, dans la rubrique « mode de sortie », du décès, ne soit pas communiquée ;
— les résultats publiés ne soient diffusés que sous forme de pourcentages.

Fixe à 14 mois à compter de l'obtention des données, la durée de conservation de celles-ci par la revue « Sciences et Avenir ».

Délibération n° 99-062 du 21 décembre 1999 portant autorisation de mise en œuvre par la revue « Le Figaro magazine » 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° 78774 du 17 juillet 1978 modifié et notamment son chapitre IV ;

Vu la demande d'autorisation présentée par la revue « Le Figaro Magazine » ;

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 revue « Le Figaro Magazine » 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 détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1997 et en 1998 par les établissements de santé publics, y compris l'Assistance Publique des Hôpitaux de Paris et les Hospices Civils de Lyon, et une copie informatique des résumés de sortie anonymes produits en 1998 par les établissement de santé privés ;

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) 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 actes pratiqués ; qu'ainsi, l'identité des patients n'est en aucun cas communiquée ;

Considérant que l'article 40-13 de la loi du 6 janvier 1978, issu de l'article 41 de la loi du 27 juillet 1998, 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 revue sollicite l'obtention du contenu intégral des « résumés de sortie anonymes », pour réaliser une analyse de l'activité hospitalière tant publique que privée, dans la perspective de publier en particulier un classement, établissement par établissement, des hôpitaux et des cliniques, selon un certain nombre de critères ; qu'il serait en particulier procédé à une analyse de la technicité de certaines activités, à une analyse de la mortalité, à une étude de la notoriété des établissements et à des études portant sur les durées moyennes de séjour par pathologie, sur des pathologies et actes médicaux spécifiques ;

Considérant qu'il y a lieu de rappeler, d'une part, que « les résumés de sortie anonymes » comportent des données individuelles dont l'exploitation informatique ne permet pas, à elle seule, 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 » 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 l'information des citoyens sur l'état du système de santé en France et en particulier sur l'activité hospitalière 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 revue prévoit que les traitements seront réalisés, sous le contrôle de trois journalistes du Figaro (dont deux ont la qualité de médecins), par un sous-traitant nommément désigné ; que les données seront conservées sur un poste dédié unique, non connecté au réseau ; que trois personnes auront accès aux données (deux médecins et un statisticien) et que l'accès à l'application sera protégé par des procédures de mots de passe individuels ; qu'il importe qu'une journalisation des connexions soit mise en œuvre, de sorte que trace soit conservée de tout accès aux informations ;

Considérant qu'une clause de confidentialité sera signée entre le directeur des rédactions du Figaro Magazine et le président de la société sous traitante, qui s'engage et engage les salariés qui effectuent les traitements :
— à ne prendre aucune copie des documents et supports d'information confiés par les journalistes du Figaro Magazine, à l'exception de celles nécessaires à l'exécution du traitement ;

— à ne pas utiliser les documents et informations traités pour son propre compte ;
— à ne pas divulguer ces informations ou documents à d'autres personnes ;
— à prendre toutes mesures permettant d'éviter l'utilisation détournée ou frauduleuse des fichiers informatiques au cours de leur conservation et de leur traitement ;
— à prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de leur durée de conservation ;
— à la fin de la durée autorisée de conservation des RSA, à procéder à la destruction de tous les fichiers informatisés stockant les informations de base et les informations traitées ainsi que les supports des informations ;

Considérant que la clause doit être complétée pour prévoir l'interdiction de toute interconnexion ou rapprochement de fichiers de données directement ou indirectement nominatives ou toute information susceptible de révéler l'identité d'une personne et/ou son état de santé ;

Considérant que, sous cette réserve, l'architecture technique présentée et les engagements pris permettent de considérer que les garanties de sécurité sont sérieuses et de qualité ;

Considérant que le directeur de la rédaction du Figaro Magazine 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 ; qu'il importe que les résultats publiés ne soient diffusés que sous forme de pourcentages ;

Considérant que la revue envisage de conserver les données qui lui seraient transmises pendant une durée de 14 mois, 10 mois étant nécessaires aux analyses pour publication des résultats et 4 mois après publication pour d'éventuels traitements supplémentaires ;

Considérant, qu'au regard de la finalité poursuivie par le traitement, cette durée n'est pas excessive ;

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 que la communication de l'indication du mois de sortie, n'est pas pertinente dans la mesure où l'information sur la durée de séjour figure, en tant que telle, dans le « résumé de séjour anonyme » et sera communiquée au demandeur ; qu'au surplus elle est de nature à permettre une identification indirecte des personnes concernées ;

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 l'analyse de la notoriété des établissements de santé ne justifie pas que soient transmis l'intégralité des codes géographiques du lieu de résidence des patients, l'indication du département de résidence étant un des éléments suffisant pour mesurer l'attractivité d'un établissement ;

Considérant que la transmission systématique de l'indication relative aux décès n'apparaît, pas en l'état, pertinente dans la mesure où n'étant systématiquement remplie que pour certaines pathologies spécifiques, la fiabilité des études de mortalité projetées ne saurait reposer sur un champ informationnel n'étant pas systématiquement renseignée ; qu'en revanche lorsque, pour certaines pathologies déterminées, l'indication du décès figure dans la classification des groupes homogènes de malades, sous des codes spécifiques, la revue pourra en avoir communication ;

Considérant en conséquence que la communication par la direction des hôpitaux et par la CNAMTS des résumés de sortie anonymes devra être expurgée de l'indication, dans la rubrique « mode de sortie », du décès ;

Autorise la revue « Le Figaro Magazine » à obtenir 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 détenus par la direction des hôpitaux et par la CNAMTS, et produits en 1997 et en 1998 par les établissements de santé publics ou privés, y compris l'Assistance Publique des Hôpitaux de Paris et les Hospices Civils de Lyon et une copie informatique des résumés de sortie anonymes produits en 1998 par les établissements de santé privés, sous réserves que :
— l'indication du mois de sortie ne soit pas communiquée ;
— 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 ;
— le code géographique de résidence soit remplacé par la seule indication du département de résidence du patient ;
— l'indication, dans la rubrique « mode de sortie », du décès, ne soit pas communiquée ;
— les résultats publiés ne soient diffusés que sous forme de pourcentages ;
— la clause de confidentialité qui sera conclue avec la société sous-traitante prévoit qu'il ne sera procédé à aucune interconnexion ou rapprochement d'informations ou de fichiers susceptibles de permettre l'identification des patients et de révéler leur état de santé ;
— un dispositif de journalisation des accès aux fichiers détenus par la société sous-traitante soit installé.

Fixe à 14 mois à compter de l'obtention des données, la durée de conservation de celles-ci par le Figaro Magazine.

III. SESAM VITALE EN MARCHE

Le dispositif SESAM-VITALE (Système Electronique de Saisie de l'Assurance Maladie associé à la carte VITALE) a pour objectif premier, il convient de le rappeler, de simplifier les procédures de remboursement — l'assuré n'ayant plus à remplir et à expédier sa feuille de soins, désormais directement télétransmise par son médecin à la caisse — et de réaliser ainsi des gains de productivité dans le traitement des feuilles de soins par les caisses de sécurité sociale. Mais, dans la mesure où les feuilles de soins électroniques ont vocation à comporter le code détaillé des actes prescrits, des prestations et des pathologies, l'assurance maladie devrait également disposer, par

l'exploitation informatique de ces informations, d'un outil sans précédent de connaissance et d'évaluation des pratiques médicales et des comportements des assurés.

La CNIL suit de façon attentive la mise en place de ce dispositif et a rendu en 1996, en 1998 et en 1999 plusieurs avis sur ses différents volets (cf 17e rapport d'activité p. 251, 18e rapport d'activité p. 217 et 19e rapport d'activité p. 99). Pour se rendre concrètement de ses modalités de mise en œuvre, la Commission a procédé, au cours de l'année 1999, à plusieurs visites sur place.

A. Etat actuel du déploiement

Le déploiement du dispositif SESAM VITALE repose sur les éléments suivants :

La constitution du Répertoire national inter-régimes des bénéficiaires de l'assurance maladie (RNIAM)

Ce fichier national de l'ensemble des assurés a été créé par l'ordonnance du 24 avril 1996 pour contribuer à la diffusion des cartes VITALE et gérer les problèmes de multi-affiliations. Ce répertoire a vocation à contenir les NIR, les identités, les dates et lieux de naissance des assurés ouvrant droits comme ayant droits ainsi que l'identifiant de l'organisme qui sert les prestations d'assurance maladie à l'assuré. Le RNIAM n'a pu être immédiatement opérationnel lors de la phase de lancement de diffusion des cartes Vitale et sa montée en charge n'est à ce jour pas complètement terminée.

L'équipement informatique des professionnels de santé et l'attribution à chacun d'eux de carte de professionnel de santé — CPS — conçue à la fois comme dispositif d'identification et de signature électronique et comme clé d'accès sécurisée aux réseaux et fichiers médicaux.

L'informatisation des professionnels de santé, et en particulier des médecins s'effectue progressivement, sachant que les pharmacies et les laboratoires de biologie sont depuis longtemps largement équipés en informatique**.** En janvier 2000, 54 % des médecins libéraux avaient reçu une carte CPS (soit plus de 60 000 médecins). S'agissant des masseurs kinésithérapeutes, 31 % d'entre eux ont demandé leur CPS (74 % l'ont reçue). En ce qui concerne les pharmaciens, 36 % d'entre eux ont demandé leur CPS (la moitié l'ont reçue). Les chiffres sont encore très modestes pour les autres professions de santé, orthophonistes, infirmières, chirurgiens dentistes, dans la mesure où pour ces deux dernières professions, en l'attente d'accords conventionnels, il n'y a pas eu encore de diffusion de masse de cartes CPS.

Il est prévu à terme de diffuser plus de 1,5 millions de cartes, dont 800 000 aux professionnels de santé.

La diffusion, à l'ensemble de la population d'assurés de la carte à puce VITALE destinée à remplacer la carte d'assuré papier.

La diffusion à l'ensemble des bénéficiaires de l'assurance maladie de ces cartes doit s'effectuer en deux étapes.

La première étape, actuellement terminée, a consisté à adresser aux assurés, région par région, les cartes dites VITALE 1, cartes familiales qui comportent les mêmes informations médico-administratives que celles qui figurent actuellement sur la carte papier d'assuré social (par conséquent, la seule information confidentielle susceptible de figurer sur cette carte concerne les personnes prises en charge à 100 % au titre d'une affection de longue durée (ALD). Ces cartes attestent l'ouverture des droits à l'assurance maladie et permettent aux professionnels de santé, par une recopie automatique des informations figurant sur la carte, de renseigner en conséquence les feuilles de soins électroniques.

Dans une seconde étape, il est prévu que la carte devienne individuelle (c'est-à-dire que chaque bénéficiaire de l'assurance maladie en dispose, ouvrant droit comme ayant droit) et comporte un volet médical (cf supra).

La télétransmission des feuilles de soins électroniques.

En janvier 2000, il était estimé qu'environ 5 % des feuilles de soins étaient désormais transmises par voie électronique (plus de 900 millions de feuilles de soins papier sont adressées chaque année à la sécurité sociale).

On assiste à une progression régulière du nombre de médecins libéraux ayant recours à la télétransmission sachant que les chiffres concernant les autres catégories de professionnels de santé sont encore très modestes.

Le Réseau Santé Social (RSS), géré sous la forme d'une concession de service public par la société CEGETEL, est destiné à assurer l'acheminement des feuilles de soins électroniques et plus généralement à échanger des informations entre les professionnels de santé qui pourront également par ce moyen accéder à des bases de connaissances. De par le régime de la concession de service public, il offre des garanties de sécurité (accès réservé aux seuls titulaires de la carte CPS, authentification des professionnels de santé, traçabilité des flux…) de neutralité (contrôle des diffusions à caractère publicitaire) et de qualité (les applications mises en œuvre sur le RSS doivent être agrées par le ministère de la santé après avis d'un comité créé à cet effet). La messagerie du réseau santé social est sécurisée par un dispositif de chiffrement.

Toutefois, l'abonnement au RSS ne constitue pas une obligation pour les professionnels de santé. En revanche les caisses d'assurance maladie ne peuvent réceptionner que des feuilles de soins électroniques transmises via le RSS.

Ainsi, les professionnels de santé, dans le cadre du dispositif SESAM Vitale, peuvent télétransmettre les feuilles de soins soit en se connectant directement au réseau santé social, soit indirectement par internet en passant par un fournisseur

d'accès qui assure ensuite la connexion au RSS par un point de raccordement (passerelle de messagerie).

On assiste ainsi à un développement d'offres concurrentielles en ce domaine à l'initiative d'opérateurs de télécommunications, de sociétés de communication médicale, d'organisations professionnelles (syndicats, unions régionales de médecins...). France Télécom par sa filiale Wanadoo santé, la société Cégédim par le réseau SANTENET, Medsyn, détenu par le syndicat MG France (réseau associé au RSS) Liberalis, créé à l'initiative d'unions régionales de médecins libéraux, offrent ainsi la possibilité à leurs abonnés de télétransmettre des feuilles de soins.

Se pose à cet égard la question de l'interopérabilité entre ces différents réseaux qui à ce jour ne communiquent pas entre eux. On voit poindre le risque que les professionnels de santé confrontés à l'impossibilité de communiquer entre eux du fait de leur appartenance à des réseaux différents choisissent par commodité des outils de messagerie internet standards accessibles sans contrainte particulière.

Parmi les 121 logiciels de télétransmission agréés par le GIE SESAM Vitale, 69 permettent aujourd'hui aux professionnels de santé de transmettre les FSE sans se connecter directement au RSS.

Autrement dit, actuellement si la totalité des feuilles de soins électroniques transitent par le RSS, point de passage obligé, 30 % d'entre elles passent d'abord par internet.

Le bilan de SESAM VITALE reste donc aujourd'hui contrasté. Lors du déploiement, certaines difficultés politiques et techniques sont apparues (manque de coordination dans la mise en place des différents volets du dispositif, problèmes de compatibilité entre matériel informatique et logiciels de télétransmission...) et ont entraîné certains retards dans la mise en œuvre du dispositif dans certaines régions (notamment à Paris). Ces difficultés apparaissent donc aujourd'hui en voie de résolution.

Toutefois des réticences et des craintes se manifestent encore chez certains professionnels de santé et assurés sociaux quant au respect effectif de la confidentialité et aux modalités d'utilisation du volet de santé de la future carte VITALE 2.

B. La télétransmission des feuilles de soins : les garanties à prendre

Au début de l'année 2000, la Commission a estimé nécessaire, deux ans après la mise en place officielle de SESAM VITALE de dresser un état des mesures de sécurité mises en place. A la suite de ce bilan, la Commission a saisi le Ministère de l'emploi et de la solidarité afin d'obtenir de sa part confirmation des solutions finalement arrêtées en ce qui concerne le dispositif de sécurisation des télétransmissions. Elle a également souhaité appeler son attention sur la nécessité de prévoir un encadrement tant juridique que technique de l'activité des organismes intermédiaires (« concentrateurs ») appelés à intervenir dans le traitement des feuilles de soins.

L'ordonnance du 24 avril 1996 et le décret du 30 décembre 1997 pris pour son application rendent désormais le professionnel de santé responsable du bon acheminement de la feuille de soins en cas de transmission électronique alors que jusqu'à présent c'était à l'assuré d'adresser à sa caisse sa feuille de soins par courrier.

Ce transfert de charges explique pour partie les réticences manifestées par une partie des professionnels de santé qui ont obtenu en contrepartie des compensations financières.

Outre le fait que le dispositif SESAM Vitale est souvent perçu comme un moyen de contrôle supplémentaire de leur activité, les professionnels de santé s'inquiètent également du respect effectif de la confidentialité des feuilles de soins électroniques transmises.

Qu'en est-il sur ce point ?

1) LA SÉCURISATION DES TÉLÉTRANSMISSIONS

Hors le dispositif SESAM Vitale, il existe déjà depuis plusieurs années, dans le cadre des procédures de tiers payant, des télétransmissions via le réseau commuté téléphonique entre les pharmaciens ou les laboratoires d'analyse d'une part, et les caisses d'autre part.

La CNIL a eu l'occasion de se prononcer en 1993 sur ces traitements (avis du 15 juin 1993 concernant le traitement IRIS de télétransmission des factures entre professionnels de santé et caisses primaires). Elle avait alors considéré que les sécurités applicables aux transmissions des informations effectuées via le réseau téléphonique commuté étaient satisfaisantes notamment en ce qui concerne les procédures d'identification des professionnels de santé. Elle n'avait pas exigé le chiffrement des informations transmises dont l'utilisation, il convient de le souligner, était à l'époque très strictement réglementée.

Depuis lors, la loi Teulade du 4 janvier 1993 a imposé aux professionnels de santé de transmettre aux caisses de sécurité sociale le code détaillé des actes, des médicaments et des pathologies et la Commission a eu l'occasion de se prononcer sur la mise en place du codage des actes de biologies et des médicaments, les autres nomenclatures n'étant pas à ce jour encore définies.

Or, lors de l'avis rendu le 19 décembre 1995 sur la mise en place, par la CNAMTS, du codage des actes de biologie, la Commission avait pris acte que « les télétransmissions des données nominatives de facturation enrichies des codes des actes de biologie seraient sécurisées par des dispositifs qui [...] permettraient par l'utilisation de cartes à micro-processeur, de lecteurs de cartes et de logiciels appropriés d'une part d'identifier et d'authentifier les laboratoires et les cliniques, d'autre part de certifier et de chiffrer certaines données ». La Commission avait également considéré « qu'eu égard aux risques de divulgation et d'utilisation détournée des informations, la CNAMTS devait examiner les modalités qui pourraient être mises en œuvre afin de chiffrer les données d'identification et les conséquences d'un tel

chiffrement, notamment pour les échanges de données nominatives avec les organismes complémentaires ».

Les mêmes observations ont été présentées lors de l'avis du 4 juin 1996 rendu par la Commission sur le codage des médicaments.

La généralisation des télétransmissions prévues dans le cadre du dispositif SESAM Vitale rend plus que jamais nécessaire la prise en compte de ces recommandations.

La sécurisation des flux est à ce jour assurée de la façon suivante.

La carte CPS permet l'identification et l'authentification des professionnels de santé émetteurs des feuilles de soins ainsi que la signature des feuilles (décret n° 98-271 du 9 avril 1998 pris après avis de la CNIL). Le code des actes figurant sur ces feuilles fait l'objet d'un « brouillage ».

Pour des raisons techniques, il est aujourd'hui envisagé que la fonction de chiffrement des informations, qui devait être assurée initialement par la carte, soit de préférence assurée par un dispositif implanté directement sous forme logicielle dans le poste de travail du professionnel de santé. La clé de chiffrement serait également stockée sur ce poste de travail et le professionnel de santé pourra la changer s'il a des craintes sur la perte de confidentialité. Cette solution pourrait être opérationnelle vers la fin de l'année 2000.

Compte tenu de ces nouvelles orientations, la Commission a demandé au Ministère à être saisie rapidement des dispositifs qui seront arrêtés et du calendrier de déploiement.

2) L'INTERVENTION DES ORGANISMES INTERMÉDIAIRES (« CONCENTRATEURS ») DANS LE TRAITEMENT DES FEUILLES DE SOINS ELECTRONIQUES

La transmission des feuilles de soins électroniques entre le professionnel de santé et les organismes d'assurance maladie peut être réalisée soit directement soit par l'intermédiaire d'un organisme concentrateur technique, la liaison s'effectuant alors en deux temps, du professionnel de santé vers l'organisme tiers puis de celui-ci vers le centre informatique de la caisse.

Les concentrateurs reçoivent les feuilles de soins, effectuent après traitement des informations le routage de celles-ci vers les organismes d'assurance maladie obligatoires et/ou complémentaires concernés et peuvent assurer le cas échéant le suivi technique de la bonne réception de ces informations par ces organismes.

Cette intervention des concentrateurs n'est pas nouvelle. En effet, les pharmacies confrontées depuis plusieurs années, dans le cadre des procédures de tiers payant, au problème de l'éclatement des flux de facturation entre les différents organismes payeurs, se sont pour bon nombre d'entre elles organisées pour mettre en place les structures nécessaires pour permettre la télétransmission des données à un

interlocuteur unique (concentrateur) chargé de retransmettre celles-ci aux organismes concernés.

La taille et l'activité et la nature juridique de ces organismes sont extrêmement variées. Il peut s'agir aussi bien d'une société informatique, d'un façonnier, que d'une union de moyens, d'une association, d'un GIE constitués par des professionnels de santé ou par une instance représentative de telle ou telle profession.

Toutefois, les types d'activités susceptibles d'être exercées par ces concentrateurs peuvent de façon schématique être résumés comme suit :
— ceux qui agissent pour des professionnels de santé non encore équipés de matériel informatique (ex : infirmiers) : ils gèrent la télétransmission des feuilles de soins de A jusqu'à Z, de la collecte des feuilles de soins en fin de journée à la réception des accusés de réception « logiques ».
— ceux qui agissent pour les professionnels de santé déjà équipés de matériel informatique (Pc, modem et lecteur de carte Vitale) : le professionnel de santé saisit les feuilles de soins et le concentrateur assure le contrôle du « parcours » de la FSE (réception, sauvegarde, routage, vérification des remboursements en cas de tiers payant, gestion des accusés de réception logiques transmis par les caisses…).
— ceux qui mettent gratuitement à la disposition du professionnel de santé (pharmacies ou médecins) un kit logiciel permettant non seulement de gérer le cabinet mais également de télétransmettre les feuilles de soins ou les factures subrogatoires en contrepartie d'une transmission d'informations sur l'activité de prescription.

Certains organismes concentrateurs proposent en effet aujourd'hui des offres de services complémentaires reposant sur l'exploitation pour leur propre compte des données médicales directement télétransmises par les professionnels de santé.

Jusqu'à présent, cette exploitation n'est pas opérée directement à partir des informations figurant sur les feuilles de soins, mais à partir d'autres flux de données distincts des télétransmissions de feuilles de soins électroniques, les professionnels de santé n'étant pas toujours pleinement informés des modalités de ces transmissions.

Il est important de souligner que le nombre de ces organismes connaît une croissance régulière. L'enjeu économique que représentent aujourd'hui les échanges de données de santé, incite de nombreux acteurs (organisations de professionnels de santé, sociétés de communication médicales, banques, assurances…) à prendre position sur ce marché.

Ces organismes doivent faire l'objet d'un attention particulière dans la mesure où ils reçoivent et centralisent des informations nominatives sensibles et… « convoitées ».

La Commission a dès 1993 pris position sur ce sujet. Lors de l'avis rendu le 15 juin 1993 sur la mise en œuvre par la CNAMTS de procédures de télétransmission des factures entre professionnels de santé et caisses primaires, la CNIL a en effet rappelé que « ces organismes ne devaient assurer aucun traitement particulier pour leur propre compte, n'effectuer ni enrichissement, ni consultation hormis celles rendues nécessaires par la maintenance des matériels utilisés, ni cession des informations ».

Cette exigence a été rappelée lors de l'avis rendu en 1996 sur la mise en œuvre du codage des médicaments, ainsi que dans la délibération n° 98-027 du 24 mars 1998 portant avis sur le projet d'arrêté relatif aux conditions de réception et de conservation des FSE.

En 1996, s'inquiétant de la légalité de l'activité des concentrateurs et des risques d'utilisation détournée des informations ainsi transmises, constatant que l'intervention de ces organismes n'était prévue que dans le cadre d'accords conventionnels locaux conclus entre les caisses et les professionnels de santé, la CNIL avait déjà appelé l'attention du Ministère des affaires sociales sur l'opportunité d'un encadrement juridique de cette activité.

Le Ministère, tout en estimant que l'activité des concentrateurs n'était pas en soi illégale, avait souscrit à la proposition de la CNIL en évoquant la possibilité de prévoir sur ce point des avenants aux conventions nationales conclues avec les professionnels de santé et des « règles déontologiques, à traduire en textes réglementaires ou à tout le moins en règlement de réseaux ».

Compte tenu de la sensibilité des informations ainsi transmises et traitées, la Commission estime aujourd'hui nécessaire de prévoir une réglementation en ce domaine, qui pourrait notamment se traduire par des dispositions dans les conventions nationales avec les professionnels de santé prévues au titre de l'article L 161-34 du code de la sécurité sociale.

Certaines des recommandations formulées par la CNIL en 1993, lors de l'avis rendu sur la mise en œuvre par la CNAMTS de procédures de télétransmission des factures entre professionnels de santé et caisses primaires, pourraient utilement servir de base à ces dispositions conventionnelles. La Commission avait alors précisé que les organismes concentrateurs ne devaient assurer aucun traitement particulier pour leur propre compte, n'effectuer ni enrichissement, ni consultation hormis celles rendues nécessaires par la maintenance des matériels utilisés, ni cession des informations.

Un tel encadrement juridique, que la CNIL appelle de ses vœux, devrait également être assorti d'obligations de sécurité particulières.

Il n'est en effet pas inutile de rappeler que l'article 1er de l'arrêté du 9 avril 1998 relatif aux conditions de réception et de conservation des FSE prévoit que lors de chaque transmission, les feuilles de soins électroniques soient transmises dans des conditions qui interdisent la lecture des données confidentielles par un tiers lors de son acheminement.

C. Le volet médical de la carte Vitale : l'état des réflexions

La mise en place de la deuxième étape du dispositif VITALE, à savoir l'attribution à chacun d'une carte de santé — la future carte VITALE 2 — offre l'occasion de renouveler la réflexion sur les droits des malades. Le débat parlementaire sur le projet de loi relatif à la couverture maladie universelle en a été l'occasion. La CNIL se ré-

jouit également de l'annonce faite récemment par le Premier Ministre d'un prochain projet de loi sur les droits des malades consacrant, en particulier, au moins dans son principe la reconnaissance d'un droit d'accès direct au dossier médical.

Lors de l'examen des projets expérimentaux de cartes de santé lancées en France dans le milieu des années 80, la Commission a en effet toujours rappelé, dans ses avis, la nécessité de recueillir l'accord des patients et de leur garantir la maîtrise des informations figurant sur la carte, le contenu de celle-ci devant être porté à leur connaissance.

L'examen du projet de loi relatif à la couverture maladie universelle et en particulier de l'article additionnel relatif au volet médical de la carte VITALE a ainsi été l'occasion pour la CNIL de rappeler dans son avis du 18 février 1999 ces deux impératifs.

La Commission a notamment estimé que l'enregistrement des informations médicales dans le volet de la carte ne devait s'effectuer qu'après accord du titulaire de la carte et qu'aucune copie papier du volet médical ne devait être délivrée aux patients afin que nul ne puisse exiger de celui-ci, dans des circonstances étrangères à la relation de soins, la production d'un « certificat de bonne santé ». Il s'agit tout particulièrement d'éviter que des employeurs ou des compagnies d'assurance puissent exiger d'un candidat à l'emploi ou d'un souscripteur une copie du volet médical. Le même type de précautions existe déjà pour les relevés des condamnations ou encore pour le nombre de points restant sur le permis à points ou encore pour les inscriptions au fichier des incidents de paiement tenu par la Banque de France.

Le texte finalement adopté par le Parlement (article 36 de la loi du 27 juillet 1999 portant création d'une couverture maladie universelle) suit les recommandations de la CNIL et privilégie les libertés individuelles et les droits des usagers.

Ainsi, aucune information médicale ne sera portée dans la carte sans que son titulaire n'en ait eu connaissance et ait donné son accord à cet effet. Il est également prévu que le décret en Conseil d'Etat qui sera pris en application de la loi fixe notamment les catégories d'informations dont il ne pourra être délivré copie. Ce décret sera pris après avis motivés et publics de la CNIL et de l'Ordre des médecins.

Le droit de faire rectifier ces informations, et, le cas échéant, de les faire supprimer, est réaffirmé.

Enfin, l'usager pourra conditionner l'accès au contenu de la carte à la frappe d'un code secret.

Reste un certain nombre d'interrogations qui devront être tranchées lors de l'examen du projet de décret d'application de la loi dont la CNIL sera saisie, qu'il s'agisse en particulier du contenu de la carte, de ses modalités d'accès par les professionnels de santé et par les usagers eux-même.

Ainsi, doit-on prévoir que les patients ne pourront exercer leur droit d'accès et consulter le contenu de leur carte que chez un professionnel de santé disposant du matériel de lecture et d'une carte d'habilitation, ce qui permettrait au médecin de donner ainsi toutes les explications nécessaires mais obligerait le patient, s'il

souhaite exercer son droit d'accès en dehors d'une consultation « normale » à prendre spécifiquement rendez vous et à devoir acquitter le prix de cette « intervention » ?

Doit-on élargir ces modalités d'accès et prévoir la consultation des informations sur des bornes publiques, par exemple dans les locaux de la sécurité sociale ou même depuis le domicile ?

En tout état de cause, dès lors que l'on conçoit le volet médical de la carte VITALE comme un « aide mémoire » de santé, établi au seul bénéfice de l'usager, il serait paradoxal qu'il ne puisse disposer de toutes facilités pour consulter le contenu des informations y figurant.

Ce texte devra également détailler le contenu et les modalités d'inscription et de consultation des données par les professionnels de santé, points qui ne font pas aujourd'hui l'objet d'un réel consensus. Certains s'interrogent même sur l'utilité d'inclure des informations médicales détaillées dans la carte VITALE à l'heure du développement des réseaux et de la possibilité d'accéder en temps réel à l'information, même lorsqu'elle est stockée en des lieux différents. La carte ne pourrait-elle pas alors être conçue comme un « Sésame » permettant à un professionnel de santé de recueillir, avec l'accord du patient, des informations complémentaires auprès d'un confrère dont l'adresse électronique aurait été enregistrée dans la carte ?

Le débat n'est pas clos.

Certaines questions méritent encore réflexion.

QUEL RECENSEMENT POUR DEMAIN ?

L'année 99 aura été une année de recensement général de la population (RGP), celui-ci constituant la plus vaste opération de collecte de données personnelles et revêtant, en application de la loi n° 51-711 du 7 juin 1951, un caractère obligatoire.

Comme lors des précédents recensements, l'INSEE, en concertation avec la CNIL, avait établi les modalités de la collecte de manière à garantir la confidentialité des réponses qui sont couvertes par le secret statistique. Les données recueillies sous la responsabilité de l'INSEE ne peuvent en effet être exploitées que par l'Institut et à des fins exclusivement statistiques. Elles ne peuvent pas être communiquées à d'autres administrations — en tout cas sous leur forme nominative — et ne doivent pas être exploitées par les services communaux qui participent aux opérations de recensement. Ceux-ci, dès le recensement de 1990, se sont vu interdire par la CNIL, en accord avec l'INSEE, l'exploitation à quelque fin que ce soit des données collectées. En contrepartie, l'INSEE s'était engagé à mettre à la disposition des mairies les premiers résultats statistiques du recensement plus rapidement que lors du recensement de 1982, ce que permettait la modernisation des techniques d'exploitation (cf 10e rapport d'activité, p 108).

C'est un dispositif de même nature que la Commission a arrêté, en accord avec l'INSEE, pour le RGP de 1999. L'avis de la CNIL du 24 mars 1998 précise en effet que les données recueillies « ne peuvent donc en aucun cas être exploitées par les services communaux qui participent aux opérations de collecte et en particulier, aucune photocopie des questionnaires ne doit être faite ; les personnes procédant à de tels agissements, contraires tout à la fois aux dispositions de la loi du 7 juin 1951 et à celle de la loi du 6 janvier 1978, ainsi qu'aux dispositions de l'article 226-21 du nouveau code pénal encourraient des sanctions pénales » (cf 19e rapport d'activité, p 137). Cet avis a été rappelé dans une circulaire interministérielle du 26 novembre

1998 adressée aux préfets. Deux visites techniques ont été par la suite effectuées par la direction informatique de la CNIL au printemps 1999 auprès des centres informatiques de scannérisation et de traitement des questionnaires afin de vérifier les mesures de sécurité prises.

Le dispositif de cession des données qui avait été arrêté pour le recensement de 1990 a été revu en outre sur plusieurs points dans le souci de mieux concilier les besoins des utilisateurs et la protection de la vie privée. Ainsi, le niveau d'agrégation des résultats se présentant sous la forme de fichiers détails (c'est-à-dire de questionnaires individuels comportant pour tout élément d'identification la zone géographique dans laquelle est située l'adresse de la personne ayant répondu), a été porté de 5000 à 50 000 habitants, afin d'empêcher une réidentification des personnes par croisement de fichiers d'adresses. Les résultats statistiques présentés sous la forme de « fichiers-tableaux » (il s'agit alors de simples comptages avec ventilation selon différents critères), lorsqu'ils ne comportent pas de données sensibles, c'est-à-dire de données relatives à la nationalité ou aux migrations, au niveau de la commune, quelque soit sa taille ou au niveau infracommunal d'un quartier fixe d'environ 2000 habitants, pourront être disponibles, mais ils comporteront des données relatives aux nationalités ou aux migrations, ils seront agrégés au niveau communal ou, pour les communes de plus de 5000 habitants, au niveau des zones infracommunales prédéterminées par l'INSEE d'environ 6000 habitants (cf 19e rapport d'activité 1998, p. 141).

I. LES ENSEIGNEMENTS DU RECENSEMENT GÉNÉRAL DE LA POPULATION DE 1999

Les opérations de recensement général ont débuté le 8 mars 1999. La Commission a décidé, comme elle l'avait fait lors du recensement de 1990, de réaliser des missions de contrôle auprès de plusieurs communes afin de s'assurer des conditions dans lesquelles se déroulaient ces opérations.

Délibération n° 99-010 du 9 mars 1999 décidant des vérifications sur place auprès de différentes mairies à l'occasion du recensement général de la population

La Commission nationale de l'informatique et des libertés,

Vu la Convention 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° 51-711 du 7 juin 1951,

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

Vu la délibération nº 98-023 du 24 mars 1998 portant avis relatif à la création de traitements automatisés à l'occasion du recensement général de la population de 1999 ;

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

Considérant que la collecte des données du recensement général de la population, réalisée sous le contrôle de l'INSEE, est assurée avec la participation des mairies ; que les opérations de collecte débuteront le 8 mars 1999 pour s'achever le 3 avril 1999 ; que les questionnaires du recensement devront être adressés à l'INSEE avant le 23 avril 1999 par les mairies de moins de 10 000 habitants et en mai 1999 par les mairies de plus de 10 000 habitants ;

Rappelle que les mairies ne sont pas destinataires des données qui sont recueillies à l'occasion du recensement, couvertes par le secret statistique ; que ces données ne peuvent donc en aucun cas être exploitées — fût-ce sous forme anonyme — par les services communaux qui participent aux opérations de collecte et qu'en particulier aucune photocopie des questionnaires du RGP ne doit être faite ; que de tels agissements, contraires tout à la fois aux dispositions de la loi du 7 juin 1951 et à celles de la loi du 6 janvier 1978, sont réprimées par l'article 226-21 du nouveau code pénal ;

Rappelle que la règle du secret statistique est, pour l'Etat, la condition de la sincérité des réponses et donc de la fiabilité du recensement et, pour les personnes interrogées, la garantie que leurs réponses ne seront pas exploitées à des fins étrangères à celles, exclusivement statistiques, pour lesquelles elles sont collectées ;

Considérant qu'il convient de s'assurer que les conditions de collecte des informations recueillies à l'occasion du recensement général et les conditions dans lesquelles les mairies conserveront les questionnaires avant qu'ils soient adressés à l'INSEE respectent ces garanties.

Décide :
— de procéder à des vérifications sur place auprès des communes dont la liste suit.

C'est ainsi que quinze missions ont eu lieu du 29 mars au 17 mai 1999 auprès de communes choisies en fonction de leur nombre d'habitants, de leur situation géographique et socio-démographique ainsi que de la couleur politique de leur majorité municipale. Ont fait, sur la base de ces critères, l'objet d'une mission de contrôle les communes suivantes : Caen (115 624 hab.), Noisy-le-Sec (36 309 hab.), Strasbourg (251 545 hab.), Paris 20e, Paris 13e, Vénissieux (64 444 hab.), Orange (26 964 hab.), Avignon (89 939 hab.), Toulon (167 619 hab.), Ajaccio (59 952 hab.), Périgueux (32 848 hab.), Mantes-la-Jolie (45 087 hab.), Annecy (51 143 hab.), Cahors (19 735 hab.), Vannes (45 644 hab.).

A trois occasions, les délégations de la commission ont mis à profit ces déplacements pour rencontrer les personnels des directions régionales de l'INSEE. Tel fut le cas à Ajaccio, Caen et Strasbourg.

Ces missions avaient pour objet de vérifier que les opérations de collecte se déroulaient dans des conditions garantissant le secret statistique et le respect des dispositions de la loi du 6 janvier 1978 et particulièrement de s'assurer des moyens adoptés par les communes pour la conservation des questionnaires remplis, avant de les adresser à l'INSEE.

A l'occasion des missions de contrôle, les représentants de la Commission ont tout particulièrement examiné les modalités de recrutement des personnels chargés de la collecte, les dispositifs de sensibilisation et d'information des administrés sur le RGP, les traitements automatisés qui ont pu localement être mis en place en vue de l'exhaustivité de la collecte et les mesures de sécurité destinées à garantir la confidentialité des données.

A. Les enseignements particuliers

La Commission a pu constater que la plupart des communes contrôlées avaient recruté les agents recenseurs parmi les personnes privées d'emploi, ce qui correspondait à la philosophie générale de la circulaire interministérielle du 19 février 1999.

Elle a également relevé qu'elles avaient fait preuve d'un grand esprit d'initiative afin de préparer leurs administrés aux opérations de recensement et de faciliter la remise des questionnaires. Ainsi, parallèlement à la campagne nationale d'information menée par l'INSEE, les mairies ont beaucoup renseigné la population par des articles dans la presse locale et dans le bulletin municipal, dans le souci de rassurer et de familiariser les personnes avec leur agent recenseur. La photographie des agents recenseurs a pu, dans certains cas, et à l'initiative des communes, être publiée dans la presse avec l'indication de leur secteur d'intervention. Un numéro vert a quelquefois été mis en place afin de répondre aux questions portant sur le déroulement du recensement. Un courrier du maire expliquant les objectifs poursuivis par le RGP a été le plus souvent distribué dans les boîtes aux lettres lors du repérage des immeubles.

Plusieurs communes ont aussi mené des actions de communication sur le recensement en direction des enfants, dans le souci que ces derniers puissent, à leur tour, sensibiliser leurs parents. On citera à ce titre, l'initiative d'une commune ayant conçu une cassette-vidéo mettant en scène des enfants, qui a été diffusée dans les écoles et les centres aérés. Ailleurs, un compact-disque a été enregistré en plusieurs langues étrangères pour être diffusé par les radios locales.

Des traitements automatisés ont été mis en œuvre afin de s'assurer que les agents recenseurs affectés à tel secteur géographique avaient accompli de manière exhaustive le recensement de leur secteur. La Commission a veillé à ce qu'en aucun cas les informations portées sur les questionnaires de recensement ne soient exploitées ou enregistrées dans ces traitements. Trois des communes visitées avaient adopté ces traitements : Noisy-le-Sec, Strasbourg et Paris et respecté les préconisations de la CNIL. A Paris, les contrôleurs ont alimenté l'application mise en place par l'Atelier parisien d'urbanisme (APUR) dans chaque mairie d'arrondissement : il s'agissait

d'enregistrer les dénombrements établis par districts, à partir des feuilles de logements et des bulletins individuels distribués et collectés, afin de suivre semaine par semaine l'état d'avancement de la collecte.

De manière générale, l'impression laissée par les interlocuteurs de la Commission était celle d'une grande attention à la confidentialité des questionnaires et d'une conscience aiguë que le moindre dérapage pourrait discréditer, tout à la fois, le recensement général de la population et les équipes municipales.

Au-delà des vérifications qui ont pu être opérées dans le cadre des missions de la CNIL, cette série de visites sur place a permis aux délégations de la Commission, par les entretiens qui ont été menés avec les agents recenseurs, les fonctionnaires municipaux et les délégués INSEE, de tirer des enseignements plus généraux de ce 33e recensement général de la population.

B. Les enseignements généraux

En premier lieu, une véritable mobilisation des collectivités locales a pu être observée, au service de cette mission. Les opérations de recensement ont incontestablement été l'occasion pour de nombreuses communes de mieux connaître leur population, voire les difficultés de leurs administrés. De nombreux agents recenseurs ont fait état de situations de pauvreté, de détresse ou d'isolement dont ils n'avaient pas conscience au préalable. Certains élus ont d'ailleurs demandé aux agents recenseurs de ne pas hésiter à leur signaler les situations dont ils auraient été les témoins, dans le respect de la confidentialité des renseignements recueillis.

En deuxième lieu, plusieurs indices attestent que le recensement de 1999 a été plus difficile à réaliser que le recensement de 1990. Ainsi, le taux de retour des bulletins avant relance a été plus faible qu'en 1990 ; celui des bulletins retournés incomplets ou illisibles, plus élevé qu'en 1990. Plusieurs raisons ont été invoquées par les interlocuteurs de la Commission pour expliquer ces difficultés.

La première tient d'abord au sentiment d'insécurité de certaines personnes qui hésitent à ouvrir leur porte ou refusent, le plus souvent par crainte, de recevoir l'agent recenseur à domicile.

La deuxième raison est une plus grande réticence qu'auparavant à répondre aux questions. Beaucoup de personnes ont fait part de leurs interrogations sur le caractère anonyme du recensement, dans la mesure où leur nom, prénoms, adresse étaient collectés (l'adresse est un élément déterminant du recensement ; les nom et prénoms sont destinés à éviter les « doublons »). D'autres encore ont manifesté leur incrédulité sur l'utilisation exclusivement statistique des résultats. Ainsi, la collecte d'informations relatives au confort du logement, pourtant déjà posée à l'occasion du précédent recensement de 1990, a pu laisser penser que ces informations seraient communiquées aux services fiscaux. Dans le même esprit, de nombreuses personnes vivant maritalement, ont déclaré vivre seules, parce qu'elles redoutaient de perdre les aides qui leur étaient attribuées… D'autres disposant d'une salle de bain supplémentaire n'ont pas répondu par peur de voir leur taxe d'habitation majorée. La rubrique relative au nom et à l'adresse de l'employeur a été très contestée. Destinée à

permettre à l'INSEE d'évaluer la distance moyenne entre le domicile et le lieu de travail, elle figurait pourtant lors du précédent recensement de 90 et n'avait, à l'époque, suscité aucune inquiétude particulière.

Cette méfiance nouvelle des personnes interrogées atteste sans doute une plus grande sensibilité à la protection des données personnelles. Il est vrai que les opérations de recensement se sont déroulées peu de temps après le développement de deux débats publics, au ton parfois passionné, l'un portant sur la mise en œuvre d'un fichier de police informatisé, le STIC, l'autre sur l'utilisation du numéro d'identification au répertoire (NIR) par les administrations financières (cf 19e rapport d'activité, p 63 et p 39). Il est, en tout état de cause, significatif de constater que, l'attitude des personnes à l'égard du recensement (réticence ou volonté de répondre) trouve généralement son explication dans une commune conviction que les résultats du recensement seront exploités par d'autres services de l'Etat !

Ainsi, les personnes vivant en centre-ville ont-elles manifesté beaucoup de réticence à répondre à certaines questions alors que des familles plus défavorisées, domiciliées généralement à la périphérie urbaine, ont répondu avec une grande rigueur. Dans un cas comme dans l'autre, c'est le sentiment que les résultats du recensement pourraient être exploités à des fins autres que statistiques qui a pu déterminer ces comportements, les uns redoutant l'exploitation que pourraient en faire les services fiscaux, les autres espérant que leur situation serait portée à la connaissance des services sociaux.

De nombreux interlocuteurs de la Commission ont signalé que les étrangers résidant en France et les habitants vivant dans des quartiers dits « difficiles » se sont prêtés avec facilité aux opérations de recensement. La collecte des données dans ces deux cas, s'est effectuée rapidement et sans problème, le recensement étant alors perçu comme un moment d'échange particulier, et un peu exceptionnel, par des personnes qui peuvent avoir ordinairement le sentiment qu'elles comptent moins que les autres. Ce dénombrement général leur restituait un sentiment d'égalité.

En définitive, la Commission n'a constaté aucun manquement aux dispositions de la loi du 6 janvier 1978 mais a nettement perçu les difficultés matérielles désormais rencontrées par les agents recenseurs pour contacter les personnes à recenser et sans doute une méfiance nouvelle de nos concitoyens à livrer à l'Etat des informations les concernant.

C'est ce constat qui, sans doute, a conduit l'INSEE à envisager de nouvelles modalités de recensement de la population.

II. LES PERSPECTIVES : UNE PROCÉDURE RENOVÉE

Lourdeurs de mise en œuvre, coût, exigeante mobilisation des communes, fortes réticences des personnes à l'égard d'une vaste opération de collecte de données entreprise par l'Etat, plus grande méfiance à l'égard de l'usage qui pourrait être

fait des données collectées : les arguments ne manquent pas qui ont pu inciter l'INSEE à envisager une nouvelle procédure de recensement.

Bien qu'elles n'aient pas été définitivement arrêtées, les grandes lignes du projet envisagé par l'INSEE sont suffisamment novatrices pour mériter d'être exposées dans ce rapport d'activité. Elles ont fait l'objet d'une saisine, pour avis, du Conseil d'Etat et de plusieurs réunions d'étude avec la CNIL. La Commission a d'ailleurs souhaité procéder à l'audition du directeur général de l'INSEE sur le schéma envisagé. Monsieur Paul Champsaur a été entendu en séance plénière le 9 décembre 1999.

A. Un projet novateur

1) UN RECENSEMENT À DEUX VITESSES OU DU RECENSEMENT AU SONDAGE

Les communes de moins de 10 000 habitants continueraient à faire l'objet d'un recensement classique mais ne seraient plus recensées simultanément : chaque année une commune sur cinq le serait, le recensement étant réparti sur l'année, hors période de vacances scolaires.

Les communes de plus de 10 000 habitants feraient désormais l'objet d'une procédure de dénombrement de la population par sondage. Chaque année, la collecte porterait sur 8 % des logements, échantillon qui serait également réparti sur l'ensemble du territoire de la commune.

2) L'EXTRAPOLATION DES RÉSULTATS ANNUELS

Chaque année, l'INSEE procéderait à l'extrapolation des résultats obtenus. En ayant recours, d'une part à un répertoire national des immeubles tenu à jour (dénommé « RIL », pour répertoire des immeubles localisés) et, d'autre part, à un outil de référence sur la structure des populations par commune ou par quartier continu d'environ 2000 habitants (dénommé « IRIS 2000 ») qui est l'actuel niveau d'agrégation minimal pour la diffusion de données statistiques issues du recensement.

Le RIL qui se présenterait comme un fichier d'adresses de logements comporte pour chaque immeuble les informations suivantes : adresse postale, nombre de logements connus, éventuellement nombre d'étages et nombre de logements par étage, mais aucune donnée sur des personnes physiques. Il pourrait être mis à jour en cas de création de nouveaux logements à partir des fichiers de permis de construire et de démolir, de la taxe d'habitation et d'autres fichiers dits « adressés » (eau, gaz, électricité etc.), mais le nom des personnes ne serait pas communiqué à l'INSEE dans le cadre de la mise à jour du RIL.

L'extrapolation des résultats d'une commune à l'autre ou d'un quartier de ville à l'ensemble de la ville nécessiterait la connaissance de la structure de population par logement, agrégée soit à une zone géographique de 2000 habitants (quartier IRIS), soit à la dimension de la commune.

Pour ce faire, l'INSEE envisage de se faire communiquer par les caisses primaires d'assurance maladie à partir de leurs fichiers de gestion, pour chaque bénéficiaire, son sexe, son année de naissance et son adresse.

Ainsi serait constitué un fichier dépourvu de caractère nominatif et qui permettrait, pour chaque quartier de 2000 habitants de disposer de la structure de la population y vivant en nombre, âge et sexe. Ce fichier à usage purement interne serait l'outil de l'extrapolation des résultats.

3) LA PROTECTION DE LA CONFIDENTIALITÉ DES DONNÉES

L'INSEE fait valoir que la nouvelle procédure peut être caractérisée par trois facteurs d'amélioration :
— la collecte étant désormais répartie sur cinq ans et concernant de plus petits volumes, les données ne seraient conservées par l'INSEE, sous leur forme nominative, que deux à trois mois.
— les bulletins de recensement seraient directement remis par les agents recenseurs à l'INSEE sans avoir à être stockés dans les mairies.
— toute personne pourrait, si elle le souhaite, adresser directement à l'INSEE le bulletin qu'elle a rempli.

Les mairies continueraient à être étroitement associées aux opérations de recensement notamment pour veiller à en assurer l'exhaustivité à partir du répertoire d'immeubles localisés que l'INSEE mettrait à leur disposition. L'INSEE qui fait valoir qu'aux Etats-Unis, pays dépourvu du maillage communal qui existe en France, le recensement coûte, par habitant, cinq fois plus cher que le recensement français, pour une qualité inférieure, se déclare très attaché à la collaboration des communes.

B. De nécessaires garanties

C'est semble-t-il un paradoxe que de constater qu'une plus grande confidentialité des données collectées est attendue des nouvelles modalités de recensement qui reposent pourtant en partie sur « l'interconnexion » de fichiers publics, ou pour le moins sur de nouveaux échanges d'informations entre fichiers.

C'en est un autre — mais seulement, celui-là, compte tenu des prouesses de calculs liées aux nouvelles technologies — que de présenter un sondage sur échantillon comme plus fiable qu'un recensement exhaustif. C'est sans doute que la science de l'aléa qui est celle des sondages et de la statistique l'a emporté définitivement (?) sur les vicissitudes de l'échange ou l'impondérable de la rencontre. Il conviendra, à défaut de désespérer tout à fait de cette tendance à l'œuvre dans bien des domaines, de maîtriser ses prolongements.

Si l'ensemble du dispositif doit reposer sur la constitution d'un nouveau fichier national d'adresses (le RIL), éventuellement mis à la disposition de l'ensemble des administrations et, le cas échéant, des entreprises privées, il y aura lieu d'en préciser minutieusement les usages possibles. C'est le sens des observations que la CNIL a porté à la connaissance de l'INSEE sur les trois points suivants.

En premier lieu, les incidences des futures modalités de recensement notamment sur la révision des circonscriptions électorales et le financement des collectivités locales imposent des modalités de mise en œuvre insusceptibles de soulever quelque contestation que ce soit sur l'authenticité des chiffres de la population.

En deuxième lieu, la commission a estimé, en l'état, que la transmission à l'INSEE d'extraits non nominatifs des fichiers des caisses primaires d'assurance maladie nécessite, compte-tenu du principe de finalité des fichiers et de l'ampleur de l'opération, l'adoption d'une loi qui devrait énumérer les seules informations strictement nécessaires à l'extrapolation des résultats et imposer que les données ainsi communiquées soient agrégées par l'INSEE à un niveau géographique de nature à éviter toute réidentification des personnes.

Enfin, si la constitution d'un répertoire d'adresses et son utilisation par l'INSEE dans le cadre de la procédure révisée de recensement n'appellent pas d'objection de fond de la part de la commission, une éventuelle diffusion de ce répertoire à des opérateurs publics ou privés mérite une réflexion approfondie et une attention vigilante, notamment sur les conditions dans lesquelles pourraient être contrôlés et encadrés de manière effective les usages possibles d'un tel fichier par des tiers.

GESTION DES RESSOURCES HUMAINES : HALTE AUX DÉRIVES !

Plusieurs affaires spectaculaires, le plus souvent portées à la connaissance du public par la presse ou par des syndicats de salariés, ont mis à jour la tentation de certaines entreprises d'aller, dans la connaissance du candidat à l'embauche ou dans la surveillance du salarié au travail, très largement au-delà de l'admissible. De telles dérives, d'autant plus regrettables que l'état du marché du travail peut dissuader les salariés de les dénoncer avec la vigueur souhaitable, ne sont pas nouvelles mais paraissent plus nombreuses.

Par ailleurs, l'introduction massive des nouvelles technologies dans l'entreprise et les traces qu'elles génèrent peuvent faire du salarié, un salarié sous surveillance.

La loi « informatique et libertés » établit, heureusement, une « règle du jeu » qui a d'ailleurs trouvé des prolongements particuliers dans le code du travail depuis la loi du 31 décembre 1992 dite « loi Aubry ».

I. RECRUTEMENT : QUI A LE PROFIL ?

A. Droit et pratique... comparés.

Le lien de subordination du salarié à l'égard de son employeur se noue bien avant que la porte de l'atelier ou du bureau ne soit franchie. Dès le stade de l'entretien d'embauche, le déséquilibre se fait jour entre le candidat à l'emploi et son éventuel futur employeur ou la société de recrutement. C'est la raison pour laquelle, dès 1985, la CNIL a adopté une recommandation de portée générale relative à la collecte et au traitement d'informations nominatives lors d'opérations de conseil en re-

crutement qui détermine le cadre juridique applicable en vertu de la loi du 6 janvier 1978 (cf 6e rapport d'activité, p 133).

A la suite des travaux de la CNIL et du rapport du Professeur Lyon-Caen, le code du travail a été complété par diverses dispositions qui constituent autant de limites fixées au rapport inégal entre employeur et candidat à l'emploi.

Ainsi, l'article L 120-2 de ce code précise que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Cette disposition, sans doute proclamatoire, présente le mérite d'afficher que l'entreprise ne saurait être un lieu de rapports exclusivement subordonnés et que les droits et libertés du salarié ou des candidats à l'emploi y ont également leur place.

S'agissant de l'embauche, l'article L 121-6 du code du travail précise que « les informations demandées sous quelque forme que ce soit au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles » et poursuit « les informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles ».

Il convient cependant de reconnaître que ces dispositions, directement inspirées des principes des législations de protection des données personnelles (principe de finalité, caractère adéquat, pertinent et non excessif des informations collectées), sont très largement méconnues.

Ainsi, il n'est pas rare qu'à l'occasion de l'accomplissement des formalités préalables à la mise en œuvre de leurs traitements de gestion des opérations de recrutement, les entreprises déclarent à la CNIL, sans doute de bonne foi, qu'elles souhaitent enregistrer la date de naturalisation de candidats français ou le mode d'acquisition de la nationalité française ou encore la nationalité d'origine !

Quelquefois, curieuses des modalités d'accomplissement du service national, les entreprises interrogent les candidats pour savoir s'ils ont été ajournés, réformés (et dans ce cas, souhaitent connaître les motifs d'exemption ou de réforme), l'année à laquelle ils ont été appelés, leur grade ou s'ils ont été objecteurs de conscience.

Il est de plus en plus fréquent que les entreprises interrogent les candidats sur leur entourage familial. Plusieurs dossiers de déclaration mentionnent à ce titre le nom, prénom, nationalité et profession des père et mère, quelques autres n'hésitant pas à recueillir les mêmes informations sur les frères et sœurs.

Bien que dépourvue à ce stade du pouvoir d'interdire, s'agissant de déclarations relevant du secteur privé, la Commission prend systématiquement l'attache de ces entreprises pour leur rappeler les prescriptions légales, et ces initiatives suffisent généralement à les convaincre de ne pas recueillir de tels renseignements.

Toutefois, cette méthode du « cas par cas » ne saurait suffire.

Aussi, la CNIL a-t-elle entrepris une série de missions de vérifications sur place auprès d'entreprises, de collectivités locales et de sociétés de recrutement dans la perspective de compléter la recommandation de 1995. A défaut en effet de disposer d'un pouvoir réglementaire en la matière, il convient, sans doute, de passer des principes généraux — assez largement méconnus — à des recommandations plus pratiques pouvant servir de guide aux employeurs et aux candidats à l'emploi afin que chacun puisse connaître ses droits.

Cependant, ce travail à portée pédagogique n'évitera ni les dérives, ni de fermes rappels à l'ordre.

B. Le rappel à la loi : les laboratoires Servier dénoncés au Parquet

L'attention de la Commission a été appelée sur les méthodes de recrutement mises en œuvre par les laboratoires Servier. Par délibération du 4 mai 1999, la Commission a décidé de contrôler sur place les fichiers et les traitements mis en œuvre par cette entreprise.

Il convient de rappeler que la Commission ne dispose aucunement du pouvoir d'opérer des perquisitions et des saisies — comme en dispose la police judiciaire. Elle peut cependant effectuer des vérifications sur place de manière inopinée dès lors qu'un avis d'intervention précisant l'objet de la vérification sur place et ses fondements légaux a été remis à la personne concernée avant le commencement des opérations.

Il a été établi que les laboratoires Servier ne disposaient pas de traitement informatique de recrutement ou de gestion du personnel. En revanche, des fichiers manuels existaient.

Lorsqu'un candidat répond à une offre d'emploi, il est convoqué pour un entretien au cours duquel il rencontre un conseiller en ressources humaines. Un questionnaire de candidature est rempli, qui est intégré dans le dossier de recrutement, lequel, si la personne est finalement recrutée, est lui-même inclus dans son dossier du personnel.

En pratique, l'entretien avec le conseiller en recrutement fait l'objet d'un résumé sur une fiche qui est intégrée dans un fichier mécanographique. Ce fichier, constitué de 50 000 fiches sur papier bristol est classé par ordre alphabétique. Chaque fiche comporte un résumé de la procédure de recrutement qu'elle ait abouti à une embauche ou non.

Chaque fiche est constituée sur le même modèle et comporte le nom, le prénom, la date de naissance de la personne, le nom du conseiller en recrutement qui l'a reçue, la date de convocation ainsi que l'issue de la procédure de recrutement : soit la date d'engagement de la personne, soit les motifs ayant conduit à son non-recrutement.

La fiche comporte également le résumé des contacts pris, avec les références professionnelles et personnelles que le candidat est invité à livrer dans le

questionnaire de candidature. La première partie de l'analyse est relative au dévouement à l'entreprise, la deuxième au caractère et à la personnalité du candidat, la troisième à la valeur professionnelle supposée de la personne. Enfin, la fiche d'analyse comporte une conclusion générale.

Ainsi, des fiches portées à la connaissance de la Commission comportaient les commentaires suivants « issue d'une famille honorablement connue, apolitique et non inféodée à une idéologie quelconque » ou encore « bien élevée, elle est non-politisée ni revendicatrice », candidat « orthodoxe, ne semble pas politisé », n'a « pas d'implications politiques ou syndicales ». Selon les laboratoires Servier ces fiches d'analyses n'étaient plus utilisées depuis fin 1997.

Parmi les motifs de refus relevés sur des fiches directement consultées sur place par la Commission, figuraient notamment les annotations suivantes : « un peu mémère », « profil pas clair », « difficilement intégrable, taille physique », « immature », « nunuche, mais pas bête ». Une des fiches consultée comportait la mention « pas le profil (homosexuel) ».

La Commission a relevé que cette dernière appréciation relative aux mœurs de la personne était contraire aux dispositions de l'article 31 de la loi du 6 janvier 1978 applicable aux fichiers manuels.

C'est pourquoi la Commission a estimé devoir, en application de l'article 21-4 de la loi du 6 janvier 1978, porter ces faits à la connaissance du Parquet de Nanterre. A la date de rédaction du présent rapport, la suite judiciaire donnée n'avait pas été portée à la connaissance de la Commission.

Délibération n° 99-034 du 8 juillet 1999 relative aux suites à donner à la mission de contrôle sur place effectuée auprès des laboratoires Servier et portant dénonciation au parquet

La Commission Nationale de l'Informatique et des Libertés ;

Vu la Convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et notamment ses articles 21, 25, 31 et 45 ;

Vu le code du travail et notamment ses articles L 121-6 et L 122-45 ;

Vu les articles 225-1 et 225-2 ainsi que les articles 226-19 et 226-23 du code pénal ;

Vu le décret nº 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Après avoir entendu Monsieur Hubert BOUCHET, Vice Président Délégué, en son rapport et Madame Charlotte-Marie PITRAT, Commissaire du Gouvernement, en ses observations ;

Considérant que par délibération du 4 mai 1999 la Commission a décidé d'effectuer une mission de contrôle sur place des fichiers et traitements mis en œuvre par les Laboratoires Servier ; que la délégation de la Commission s'est rendue dans les locaux des Laboratoires Servier situés 22 rue Garnier 92200 Neuilly-sur-Seine le 27 mai puis le 4 juin ;

Considérant qu'il a été constaté que les laboratoires Servier n'ont mis en œuvre aucun traitement automatisé d'informations nominatives relatif au recrutement ou à la gestion du personnel ; qu'en revanche un fichier manuel comportant 50 000 fiches de candidatures, classées par ordre alphabétique, a été constitué ;

Considérant que chaque fiche comporte le nom, le prénom, la date de naissance de la personne, le nom du conseiller en recrutement qui l'a reçue, la date de convocation ainsi que l'issue de la procédure de recrutement, soit la date d'engagement de la personne, soit les motifs ayant conduit à son non recrutement ;

Considérant que ce fichier est géré par une seule personne à laquelle tous les conseillers en ressources humaines font appel lorsqu'une procédure de recrutement est engagée afin de savoir si le candidat a précédemment postulé à un emploi auprès du groupe Servier, quelle suite a été réservée à cette candidature ainsi que les motifs du non recrutement ;

Considérant qu'au titre des motifs de refus d'embauche, la Commission a constaté à partir d'une consultation d'un échantillon de 300 fiches des motifs tels que « un peu mémère », « profil pas clair », « difficilement intégrable, taille physique » ;

Considérant qu'une des fiches consultée, rayée de bleu, comportait pour seule mention aux côtés du nom et de l'adresse de la personne concernée et du poste d'« aromaticien senior » proposé : « pas le profil (homosexuel) » ; que la délégation de la Commission ayant demandé que le dossier auquel renvoyait cette fiche lui soit présenté, il lui a été exposé que ce dossier avait été détruit conformément à une note interne en date du 9 novembre 1987 aux termes de laquelle les dossiers des candidats non recrutés devaient être aussitôt détruits s'ils se rapportaient à une fiche rayée en rouge, ce code signifiant « à ne pas recruter et à ne même pas revoir en cas de nouvelle candidature » ou ne devaient pas être conservés au-delà d'une durée maximale de deux ans s'ils se rapportaient à une fiche rayée de bleu, couleur signifiant « à ne pas recruter dans l'immédiat, à revoir en cas de nouvelle candidature » ; que la fiche litigieuse ayant été établie en 1995, il était conforme à cette note interne que le dossier s'y rapportant ne fût pas conservé ;

Considérant que l'annotation « pas le profil (homosexuel) » est contraire aux dispositions de l'article L 122-45 du code du travail aux termes duquel « aucune personne ne peut être écartée d'une procédure de recrutement (...) en raison de son origine, de son sexe, de ses mœurs, de sa situation de famille, de son appartenance à une ethnie, une nation, une race, de ses opinions politiques, de ses activités syndicales ou mutualistes, de ses convictions religieuses ou (...) en raison de son état de santé ou de son handicap » ; qu'un refus d'embauche fondé sur un tel motif constitue une infraction prévue par l'article 225-2 du code pénal ;

Considérant que cette fiche ayant été établi en 1995, le délit de discrimination à l'embauche en raison des m œurs d'une personne est prescrit ; mais considérant qu'en ayant collecté et conservé dans un fichier manuel en méconnaissance des dispositions de l'article 31 de la loi du 6 janvier 1978 une donnée faisant apparaître les mœurs des personnes, Les Laboratoires Servier ont commis l'infraction prévue par l'article 226-19 du code pénal que l'article 226-23 du même code rend applicable aux fichiers manuels, infraction non prescrite ;

Considérant que l'infraction paraît constituée dans tous ses éléments et qu'elle est de nature à révéler un comportement discriminatoire à l'embauche, contraire à l'ordre public ;

Considérant, par ailleurs, que deux fiches d'analyse de candidature dits « fiche d'analyse objective » ont été adressées à la commission par une personne ayant souhaité conserver l'anonymat ; que la commission a transmis ces fiches aux Laboratoires Servier afin de recueillir leurs observations ; que les Laboratoires Servier ne contestent pas l'authenticité de ces fiches mais font valoir que les fiches transmises à la Commission ne sont « nullement représentatives » de la méthode d'analyse et, que, de surcroît, ces fiches ne sont plus utilisées depuis 1997 ;

Considérant que compte-tenu de la nature des commentaires figurant sur ces fiches, la Commission juge utile qu'elles soient portées à la connaissance du parquet ;

Décide en application de l'article 21 4° de la loi du 6 janvier 1978 de dénoncer les faits au parquet.

II. LA CYBERSURVEILLANCE DES SALARIÉS EN ENTREPRISE

A. La surveillance cantonnée par le droit

La loi du 31 décembre 1992 a posé les jalons d'un droit « informatique et libertés » dans l'entreprise. Principe de proportionnalité (« nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché » — art L 120-2 du code du travail) ; consultation du comité d'entreprise lors de l'introduction de nouvelles technologies (art L 432-2) ; information préalables des salariés (art L 121-8).

Ces principes et droits font écho à la loi du 6 janvier 1978 qui impose que tout traitement de données personnelles soit déclaré à la CNIL, que les salariés soient informés de son existence et de ses caractéristiques, qu'ils aient accès aux informations les concernant.

C'est sur la base de ces principes que, dès 1984, la Commission a établi, par le biais d'une recommandation qui devait trouver son prolongement dans une norme simplifiée, des règles d'usage des autocommutateurs téléphoniques qui permettent à l'employeur de connaître les numéros de téléphone appelés par un salarié depuis son poste (cf 5e rapport d'activité, p 109 et 15e rapport d'activité, p 74).

Ces mêmes principes trouvent application en matière de vidéo-surveillance dans l'entreprise et la chambre sociale de la Cour de cassation donnera sa substance à ces principes : nul moyen de preuve ne peut être opposé par l'employeur aux salariés si ces derniers n'ont pas été préalablement informés de la mise en place de surveillance et de contrôle.

La jurisprudence de la Cour de cassation, constante depuis 1991, quelle que soit la technologie utilisée, a été encore rappelée par un arrêt du 14 mars 2000 relatif à l'enregistrement des conversations téléphoniques des salariés dans le cadre de passage d'ordres boursiers et de prises de paris sur internet : « l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail ; que seul l'emploi de procédé clandestin de surveillance est illicite ».

Mais jusqu'à présent, qu'il s'agisse d'autocommutateur téléphonique, de badges et de contrôle d'accès ou de vidéo-surveillance, la surveillance concernait principalement la présence ou la localisation physique de l'individu.

Sans doute, le développement des écoutes téléphoniques dans le milieu du travail a-t-il signé un changement. La multiplication des services par téléphone et des centres d'appels a conduit les entreprises à surveiller la qualité du service, c'est-à-dire celle de la réponse apportée par le salarié. Sur ce point, la CNIL a développé un corpus de recommandations pratiques qui paraît être très largement respecté.

Les salariés concernés doivent être prévenus, préalablement à la mise en place du système, de son existence, des conséquences individuelles qui pourront en résulter, et des périodes pendant lesquelles leurs conversations seront enregistrées. Ils doivent pouvoir disposer de lignes non-connectées au dispositif d'écoute pour toutes les conversations qui ne sont pas directement liées au motif de l'écoute, qu'elles soient privées ou professionnelles.

Les salariés doivent avoir connaissance du compte rendu de la conversation enregistrée et doivent pouvoir formuler leurs observations.

Enfin, ces enregistrements de conversations ne doivent être conservés que le temps strictement nécessaire à l'objectif poursuivi. En pratique, la bande doit être effacée dès que le salarié l'a écoutée en présence de son chef de service. La Commission estime qu'elle peut être conservée pendant une durée de l'ordre de une ou deux semaines.

Cependant, l'émergence des nouvelles technologies de communication et tout particulièrement l'introduction d'internet dans l'entreprise ouvre un nouveau champ d'interrogations.

B. La surveillance facilitée par le tout numérique

Le recours de plus en plus systématique aux nouvelles technologies de réseau a des incidences considérables sur le rapport salarial.

Progressivement, l'information dont disposent les entreprises est numérisée, quelque soit la nature de cette information. Dès lors qu'elle est informatisée et

susceptible d'accès par internet ou Intranet, des risques d'accès indus à cette information sont réels. Pour l'entreprise, les nouvelles technologies de l'information et de la communication vont naturellement poser des problèmes nouveaux en matière de sécurité dès lors que se trouvent externalisés des informations sur toute la vie de l'entreprise, ses fichiers de personnels, de gestion de commandes, de fournitures, ses secrets de fabrique, etc. Pour les salariés, la différence de nature entre les NTIC et tout ce qui précède réside en la capacité nouvelle de la technologie de conserver toutes les traces laissées par la personne connectée.

La technique pose de façon nouvelle des questions qui avaient été réglées dans un contexte ancien. Ainsi, un message électronique que le salarié a cru supprimer peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde. Et ce salarié serait abusé si nul ne lui avait exposé que le message qu'il avait reçu de son épouse pour lui demander d'aller chercher en urgence son enfant au lycée, et qu'il avait aussitôt effacé de sa messagerie, avait été conservé à son insu.

Or, l'équilibre est délicat à trouver. L'ouverture de l'entreprise sur le monde, grâce à internet, l'utilisation des réseaux d'information la rendent plus vulnérable à des attaques informatiques venues de l'extérieur. La mise en place de mesures de sécurité constitue à cet égard une garantie tant pour éviter les intrusions ou les attaques informatiques que pour protéger des documents confidentiels, des secrets de fabrique, ou encore les fichiers de l'entreprise. Or, ces mesures de sécurité auront précisément pour objet de conserver trace des flux d'information, directement ou indirectement nominatives, afin de mieux prévenir tout risque d'intrusion et de repérer l'origine des problèmes.

Par ailleurs, ces technologies qui sont tout à la fois, ergonomiques, faciles d'emploi et parfois ludiques, vont amener les entreprises à veiller à ce que leurs salariés n'en fassent pas un usage abusif, sans lien avec leur activité professionnelle. Ce contrôle de productivité du « cyber-travailleur » s'exercera d'autant plus que toute architecture en réseau a pour effet d'éloigner géographiquement le salarié de sa hiérarchie.

Il convient de le reconnaître, l'évolution est constante depuis le contremaître, personne physique repérable, chargé de contrôler la présence physique du salarié sur son lieu de travail et en activité jusqu'aux « contremaîtres électroniques » (badges) chargés du contrôle de la présence physique. S'ouvre désormais l'ère du « contremaître virtuel » pouvant tout exploiter sans que le salarié en ait toujours parfaitement conscience et permettant, le cas échéant, au delà des légitimes contrôles de sécurité et de productivité des salariés, d'établir le profil professionnel, intellectuel ou psychologique du salarié « virtuel ».

Des entreprises de plus en plus nombreuses adoptent des chartes d'information précisant les mesures de sécurité à prendre et les usages qu'il peut être fait par les salariés des nouveaux outils informatiques mis à leur disposition. L'examen de ces chartes qui sont très rarement négociées avec les représentants du personnel ou leurs syndicats, manifeste un déséquilibre patent entre les prérogatives de l'employeur et les droits des salariés.

C'est ainsi que la plupart des chartes dont la CNIL a eu à connaître prévoient que l'ensemble des données de connexions qui peuvent révéler à l'administrateur du système, ou au chef de service, ou au directeur de personnel, l'usage qui est fait de l'outil (les sites qui ont été consultés, les messages qui ont été adressés) sont conservées pendant des durées très longues et font l'objet d'analyses individualisées.

De la même façon, les salariés sont le plus souvent contraints par ces chartes à n'utiliser le courrier électronique qu'à des fins exclusivement professionnelles, certaines sociétés, notamment des filiales de groupes américains, précisant même que tout message électronique envoyé par un salarié doit être considéré comme un « enregistrement permanent, écrit, pouvant à tout moment être contrôlé et inspecté » (sic).Toutefois, il semble que les chartes rédigées de manière radicale soient d'une application en réalité plus souple. Là où une charte précise que l'utilisation de la messagerie électronique doit être exclusivement professionnelle il apparaîtrait qu'une utilisation résiduelle à des fins personnelles soit tolérée.

Cependant, les salariés demeurent encore largement ignorants des possibilités de traçage de leur activité que les nouvelles technologies offrent à l'employeur et, de fait, l'équilibre nécessaire entre contrôle légitime exercé par l'entreprise et respect des droits des salariés ne paraît pas assuré dans bien des cas.

Cet état des lieux a conduit la CNIL à entreprendre une étude d'ensemble de ces questions dans le souci de suggérer aux entreprises et aux salariés utilisateurs l'adoption d'une règle du jeu équilibrée, comme nos autorités de protection des données l'ont fait lors de l'apparition des précédentes technologies : badges, autocommutateurs, vidéosurveillance, etc.

Cette étude doit aboutir à la rédaction d'une recommandation appelant l'attention de l'ensemble des acteurs tout à la fois :
— sur les mesures techniques devant être prises pour sécuriser les architectures en réseau et tout particulièrement les fichiers de l'entreprise (analyse des connexions, firewall, proxy) ;
— sur les capacités de la technologie à produire des traces qui, rassemblées, conservées et combinées, identifieraient chacun à partir de processus intellectuels inférés de ses traces ;
— sur la nécessaire information des salariés à l'égard de l'usage que l'employeur pourrait faire des données de trafic de connexion.

Le projet de la Commission est 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 consulté durant l'année 1999 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) ainsi que les organisations syndicales des salariés (CGT, CFDT, FO, CFTC et CGC) et patronales (MEDEF et CGPME)

Cette initiative porte la marque d'une conviction : celle que l'entrée de nos pays dotés d'une législation de protection des données dans la société de l'information ne saurait se faire sans les utilisateurs de ces nouveaux outils, ni si ces outils suscitent la méfiance des salariés.

LA PROTECTION DES DONNÉES EN EUROPE ET DANS LE MONDE : CONCERTATION ET FERMETÉ

L'année 1999 aura été marquée par la poursuite des travaux engagés précédemment dans les enceintes de deux organisations internationales plus particulièrement concernées par la protection des données personnelles, le Conseil de l'Europe et l'OCDE et par une intensification des travaux nationaux entrepris par tous les grands partenaires commerciaux de l'Europe, et tout particulièrement les Etats Unis.

Chez nos grands partenaires la situation évolue très nettement. Ainsi au Japon, les experts chargés par le gouvernement d'examiner la question de la protection des données personnelles ont remis un pré-rapport en décembre 1999 préconisant l'adoption d'une loi de base destinée à établir les grands principes de la protection des données personnelles s'imposant y compris dans le secteur privé, cette loi pouvant être prolongée, selon les besoins, par des lois sectorielles ou des codes de déontologie.

Au Canada, l'examen du projet de loi destiné à réglementer les activités des secteurs privés de compétence fédérale s'est poursuivi en 1999. Il est prévu qu'il soit adopté à la fin du premier semestre 2000.

En Australie, après bien des hésitations, le gouvernement s'est engagé en décembre 1999 à déposer un projet de loi relatif à la protection des données personnelles dans le secteur privé.

Aux Etats Unis, la législation fédérale a été complétée au plan sectoriel, selon la tradition américaine, par une loi dont l'entrée en vigueur est fixée au 30 avril 2000 visant la protection des mineurs à l'égard du traitement des données personnelles sur internet qui soumet en particulier tout traitement de données relatives à des enfants de moins de 13 ans au consentement des parents et qui confère en cette matière un pouvoir réglementaire à la *Federal Trade Commission*. Les résultats de

l'initiative législative concernant la modernisation du secteur financier, adoptée le 4 novembre 1999, paraissent moins heureux dans la mesure où cette loi qui ouvre la voie à la constitution de conglomérats financiers regroupant des filiales de banque, de crédit et d'assurance se borne à prévoir, s'agissant de la protection des données personnelles, une information des personnes concernées en cas d'échange d'informations, sans reconnaître ni droit d'accès, ni droit d'opposition à la cession des données au sein de ces groupes à des fins de prospection commerciale. Le président Clinton signant cette loi s'en serait ému. Une nouvelle initiative pourrait être prise à cet égard en l'an 2000.

Enfin, le gouvernement américain et la *Federal Trade Commission* ont poursuivi leur pression sur le secteur privé pour l'inciter à une autorégulation plus rigoureuse, notamment après la révélation de plusieurs affaires, de nature et de portée différentes, qui ont ému l'opinion américaine et parfois mondiale.

Ainsi en février 1999, l'insertion par la société Intel dans les Pentium III des ordinateurs d'un numéro unique de série pouvant être transmis, à l'insu des usagers, à des services en ligne a été dénoncée par les associations de défense de la vie privée, la procédure d'identification ayant été ultérieurement modifiée par Intel pour la placer sous le contrôle de l'utilisateur. Il convient de souligner que cette société, consciente de l'impact international de l'affaire s'est rapprochée, dans sa recherche de solution, des commissaires européens à la protection des données et notamment de la CNIL.

Quelques semaines après ce fut à Microsoft d'être stigmatisé par une partie des internautes à l'occasion de la mise en place de son nouveau système d'exploitation, modifié depuis lors, qui émettait des informations à l'insu des personnes concernées vers le site de cette société.

Depuis l'automne 1999, la société RealNetworks, éditrice du principal logiciel pour séquence vidéo « RealJukebox », fait l'objet de procès aux Etats-Unis. Il lui est reprochée d'avoir recueilli, à l'insu des internautes, des informations sur l'usage qu'ils faisaient du logiciel.

Constatant les insuffisances de l'autorégulation, des associations américaines de défense de la vie privée, et une partie de la presse américaine, telle le journal Business Week, se font régulièrement les défenseurs d'une approche législative à l'européenne, et plusieurs Etats annoncent leur intention de légiférer sur des aspects sectoriels mais de plus en plus nombreux.

S'agissant des organisations internationales, le Conseil de l'Europe devrait avoir prochainement achevé le programme engagé qui visait, d'une part, à permettre l'adhésion de la Communauté européenne à la convention 108, et d'autre part, selon la philosophie de la directive européenne, à compléter cette convention par des dispositions faisant obligation aux Etats signataires de mettre en place des autorités indépendantes de contrôle et de prévoir des garanties en matière de flux de données entre Etats-parties à la convention et Etats non parties à la convention. L'OCDE a poursuivi l'étude des solutions contractuelles en matière de protection des données et la mise au point d'un outil logiciel à portée pédagogique destiné aux sites

internet afin de leur permettre d'afficher la politique qui est la leur en matière de protection des données et de contribuer à l'application des lignes directrices de 1980.

Cependant, c'est l'importance des développements européens en matière de protection des données et de la vie privée et les discussions bilatérales entre l'Europe et les Etats Unis qui auront marqué l'actualité en 1999.

I. L'EUROPE DE LA PROTECTION DES DONNÉES

A l'heure de la constitution de fichiers de police européens et de l'accroissement des échanges entre partenaires, membres de l'Union européenne, la question a été posée de la nécessité d'une CNIL européenne. Ce débat se prolongera sans doute dans les mois qui viennent, en France, à l'occasion de la transposition de la directive du 24 octobre 1995.

A. Le contrôle des fichiers de police européens

1) QUELS FICHIERS ?

Le système d'information Schengen (SIS)

Le système d'information Schengen (SIS) a été créé par la Convention d'application de l'Accord de Schengen du 19 juin 1990, qui est aujourd'hui ratifiée par dix Etats : la Belgique, le Luxembourg, les Pays-Bas, l'Allemagne, la France, l'Autriche, l'Espagne, la Grèce, l'Italie et le Portugal. Le Danemark, la Finlande et la Suède ont un statut d'observateur mais leur participation effective à la « coopération Schengen » est prévue pour le second semestre 2000. La Norvège et l'Islande, qui ne font pas partie de l'Union européenne, ont signé en 1996 un accord de coopération avec les Etats Schengen qui doit être confirmé par une nouvelle décision du Conseil de l'Union européenne.

Aux termes du protocole, annexé au Traité d'Amsterdam du 2 octobre 1997, entré en vigueur le 1er mai 1999, les décisions et déclarations adoptées par les instances Schengen font désormais partie de « l'acquis communautaire ». Cependant, le Conseil de l'Union européenne a décidé, sur insistance de la France, que le système d'information Schengen continurait à relever du troisième pilier.

Le SIS est un fichier commun à l'ensemble des Etats membres de l'espace Schengen, qui centralise, sur le fondement des articles 95 à 100 de la Convention, deux grandes catégories d'informations qui concernent, les unes, des personnes, qu'elles soient recherchées par les autorités judiciaires ou qu'elles aient fait l'objet d'une mesure d'éloignement du territoire, les autres, des véhicules ou des objets recherchés ou volés. Le SIS peut être consulté, sous certaines conditions, par les

personnels qui exercent des missions de police, et par les agents qui traitent les demandes de visas ou de titres de séjour.

Ce système informatique est composé d'un système central (C-SIS), implanté à Strasbourg et placé sous la responsabilité du ministère de l'intérieur français ainsi que des bases nationales (N-SIS) qui en sont le reflet et qui sont les seules bases de données auxquelles ont accès les utilisateurs du SIS.

Par ailleurs, dans chacun des Etats membres, un bureau SIRENE a été créé. Ces bureaux ont pour mission de procéder à des consultations préalables à la création de signalements, à l'établissement d'ordre de priorité en cas de signalements multiples et à l'échange d'informations complémentaires sur la conduite à tenir en cas de « découverte » des personnes signalées. Le bureau SIRENE français, installé dans les locaux de la direction centrale de la police judiciaire du ministère de l'intérieur à Nanterre, est composé de fonctionnaires de la police nationale, de militaires de la gendarmerie nationale, de fonctionnaires des douanes et d'un magistrat.

D'un point de vue technique, et après les modifications apportées au système afin d'assurer l'intégration des pays nordiques et de passer sans difficulté l'an 2000, une refonte complète du SIS est actuellement à l'étude. Le « SIS 2 » ne devrait toutefois pas être opérationnel avant quatre ou cinq ans.

A la fin de l'année 1999, le SIS comportait plus de 9 millions de signalements. Six millions de signalements concernaient des documents d'identité, un million des véhicules et un million trois cents mille des personnes. L'Allemagne et la France étaient à l'origine de 60 % des signalements enregistrés dans le SIS.

Europol

La Convention Europol, signée le 26 juillet 1995 par les Etats membres de l'Union Européenne et entrée en vigueur le 1er octobre 1998, constitue un instrument de coopération policière européenne qui relève du troisième pilier, notamment en matière de terrorisme, de trafic illicite de stupéfiants et d'autres formes graves de criminalité internationale.

Europol est avant tout un office européen de police qui gère un système informatisé de données, installé à La Haye, comprenant, d'une part, un système d'informations, défini par le titre II de la Convention, et d'autre part, des fichiers de travail à des fins d'analyse, prévus par le titre III de la Convention.

Europol a pour mission de faciliter l'échange d'informations entre les Etats membres, en collectant, rassemblant et analysant des informations et des renseignements, puis en transmettant aux services compétents de chaque Etat membre les données qui les concernent.

A ce jour, le système d'informations, alimenté par les Etats membres n'est pas mis en œuvre. Les fichiers d'analyse, beaucoup plus complets, portent sur les activités d'organisations criminelles, telles que les réseaux de trafic de stupéfiants. Europol pourra ainsi fournir des renseignements stratégiques et élaborer des rapports généraux. A ce jour, une dizaine de fichiers d'analyse, ayant chacun un objet déterminé, est prévue.

Le système d'information des douanes (SID)

Le système d'information des douanes (SID), commun aux administrations douanières de l'ensemble des Etats membres, est à la fois régi par un règlement du Conseil (n° 515/97 du 13 mars 1997) relatif aux fraudes et irrégularités vis-à-vis des réglementations communautaires douanière et agricole et par une Convention intergouvernementale du 26 juillet 1995 sur l'emploi de l'informatique dans le domaine des douanes, actuellement en cours de ratification par les Etats, et dont l'objet est d'aider à prévenir, rechercher et poursuivre les infractions graves aux lois nationales sur la circulation des marchandises et sur le trafic illicite de stupéfiants.

Ce système n'est pas encore opérationnel.

Eurodac

Le système Eurodac a pour objet de centraliser les empreintes digitales, d'une part des demandeurs du statut de réfugié et de permettre ainsi la réalisation des contrôles liés à l'application de la Convention de Dublin du 15 juin 1990, et d'autre part, des personnes appréhendées à l'occasion d'un franchissement irrégulier d'une frontière extérieure de l'Union européenne.

La Convention créant le fichier a été négocié dans le cadre du troisième pilier. A la suite du Traité d'Amsterdam qui a inséré dans le premier pilier les questions relatives aux visas, à l'asile et à l'immigration, Eurodac relève désormais du premier pilier.

Le projet de règlement du Conseil, qui a fait l'objet d'un premier avis du Parlement européen à la fin de l'année 1999, est toujours en cours de discussion entre les Etats-membres. Sa dernière rédaction prévoit la création d'une base de données centrale placée sous la responsabilité de la Commission européenne, et la mise en place de moyens électroniques de transmission entre les Etats membres et la base de données centrale.

A ce jour, cette base de données n'est pas mise en œuvre.

2) QUELS CONTRÔLES ?

Un signalement dans un des fichiers de police européens peut avoir des conséquences très importantes pour la personne concernée et, tout particulièrement, sur sa liberté d'aller et venir.

C'est la raison pour laquelle, sous la pression des autorités nationales de protection des données, et en particulier de la CNIL, tous les textes européens régissant les fichiers de police comportent des dispositions en matière de protection des données.

Ainsi, un véritable socle juridique commun a été fondé au niveau européen. Ce socle est constitué d'une part, par la Convention 108 du Conseil de l'Europe du 28 janvier 1981, à laquelle chacun de ces textes fait référence, d'autre part, à la recommandation R 87 (15) du Comité des ministres du Conseil de l'Europe sur les

fichiers de police du 17 septembre 1987. Ce socle juridique comporte notamment la reconnaissance d'un droit d'accès aux fichiers, directement inspiré des dispositions de chacune des législations nationales, et le contrôle du fonctionnement des fichiers par des autorités indépendantes. C'est sur ce dernier point, cependant, que les situations sont plus diverses.

En effet, selon l'architecture des systèmes, le contrôle des fichiers est opéré soit par une autorité de contrôle commune (tel est le cas pour Europol) exclusivement composée de représentants des autorités de contrôle nationales (les « CNIL » des 15 Etats-membres), soit pour partie par l'autorité de contrôle commune et pour partie par les autorités nationales de protection des données (tel est le cas pour Schengen). Enfin, le contrôle des fichiers relevant du premier pilier (« Eurodac » et, pour partie, le SID), doit être confié à l'organe indépendant prévu par l'article 213B du Traité sur l'Union européenne. La Commission européenne prépare actuellement un projet de règlement qui préciserait les modalités de désignation de cet organe, qui pourrait être un commissaire à la protection des données choisi par le Parlement et le Conseil.

SCHENGEN :

Un droit d'accès exercé

Depuis l'entrée en vigueur le 26 mars 1995 de la Convention d'application des accords de Schengen, la Commission a reçu, au 31 décembre 1999, près de 500 demandes de droit d'accès aux SIS.

Les vérifications opérées par les commissaires de la CNIL, membres ou anciens membres du Conseil d'Etat, de la Cour de Cassation, de la Cour des Comptes permettent de vérifier la régularité des signalements et aboutissent dans près de 30 % des cas à la suppression pure et simple de la fiche du requérant.

L'information du requérant renforcé

A l'issue des vérifications opérées dans un fichier de police, la CNIL est tenue par l'article 39 de la loi du 6 janvier 1978 de notifier aux intéressés que « les vérifications ont été effectuées ». Cette formulation, qui ne permet pas d'expliquer aux requérants, la nature ou les résultats des investigations accomplies peut paraître très insatisfaisante (cf 19^{e} rapport d'activité, p 64). Cependant, s'agissant du système Schengen, les requérants sont plus exactement informés de leur situation.

Ainsi, la loi du 11 mai 1998 relative à l'entrée et au séjour des étrangers en France impose au ministère des affaires étrangères de motiver les décisions de refus de visa d'entrée en France qui sont fondées sur un signalement dans le SIS. Le Conseil d'Etat a estimé que, dans ce cas, les personnes concernées devaient être informées du pays à l'origine de leur signalement (Conseil d'Etat, 9 juin 1999, n° 198344). Si ces personnes entrent en outre dans l'une des autres catégories pour lesquelles un refus de délivrance de visa doit être motivé (conjoints, enfants à charge, ou ascendants de ressortissants français par exemple), le ministère des affaires étrangères leur indique le motif du refus de manière plus précise (par exemple, interdiction du territoire assortie d'une reconduite à la frontière).

La CNIL a, en outre, obtenu qu'en cas d'effacement d'un signalement opéré par un pays dont la législation nationale prévoit un droit d'accès direct, le requérant soit informé, avec l'autorisation de ce pays, que son signalement a été supprimé.

De manière plus générale, les personnes signalées dans le système d'information Schengen à la suite d'un arrêté d'expulsion ou d'une condamnation prononçant une interdiction du territoire peuvent être informées, à l'issue des investigations, des voies de recours qui leur sont ouvertes pour demander l'abrogation de la mesure prise à leur encontre.

Enfin, il est à souligner que le Conseil d'Etat a annulé une décision française de refus de délivrance de visa qui avait été motivée par un signalement « Schengen » effectué par l'Allemagne à la suite d'une demande d'asile (Conseil d'Etat, 9 juin 1999, n° 190384).La Haute juridiction a relevé que ce motif n'était pas au nombre de ceux énumérés limitativement par l'article 96 de la Convention Schengen susceptibles de justifier un signalement aux fins de non-admission,

Une autorité de contrôle commune active

L'autorité de contrôle commune (ACC) Schengen, prévue par l'article 115.1 de la Convention, est chargée d'exercer un contrôle technique du C-SIS et, de manière plus large, de vérifier l'application des principes de protection des données et des droits reconnus aux personnes fichées dans le SIS. L'ACC a été installée officiellement le 26 mars 1995, date de mise en application de la Convention. L'ACC est exclusivement composé de représentants des autorités indépendantes de contrôle des Etats Schengen (les « CNIL » des Etats Schengen).

L'ACC a souhaité renforcer les garanties d'indépendance qui lui sont reconnues par la Convention, d'une part, en instaurant le principe de l'élection de son président et de son vice-président, d'autre part en demandant, dès 1995, l'attribution d'une ligne budgétaire propre lui permettant de remplir ses missions.

La principale mission de l'ACC consiste à contrôler le C-SIS. A ce jour, deux contrôles ont été opérés, l'un en 1996, l'autre en 1999. Dans les deux cas, une équipe de contrôle a été désignée par l'ACC, associant des membres de l'autorité de contrôle commune et des experts nationaux. Un rapport a été rédigé, puis adressé pour observations au Groupe central et aux autorités françaises responsables du C-SIS. Sur ce fondement, l'ACC a fait des recommandations concernant le fonctionnement du SIS.

En outre, la Convention reconnaît à l'ACC un rôle de conseil et d'harmonisation des pratiques et doctrines nationales. C'est à ce titre, notamment, que l'ACC s'est préoccupée du problème des alias. Les personnes qui ont été victimes d'un vol de documents d'identité ou qui les ont perdus peuvent être fichées dans le SIS dans la mesure où les auteurs d'infraction peuvent avoir usurpé l'identité de leurs victimes. Or, actuellement, l'architecture du SIS ne permet pas de distinguer les personnes auteurs d'une usurpation d'identité de celles qui en sont les victimes.

Les conséquences de cette inscription sont fortement préjudiciables pour les personnes dont le patronyme est utilisé comme alias. Ainsi, il n'est pas rare que les

personnes concernées soient interpellées par les services de police à l'occasion de contrôles, ou qu'on leur refuse l'entrée sur le « territoire Schengen ». L'ACC a officiellement demandé dans un avis du 3 février 1998, que de solutions puissent être trouvées sans attendre la mise en place du SIS 2.

Dans un souci de transparence, l'ACC a décidé, alors que l'obligation ne lui en est pas faite par la Convention, d'élaborer un rapport annuel d'activité. Ce rapport, présenté lors d'une conférence de presse, est transmis aux autorités Schengen et rendu public, dans chaque pays concerné, par les autorités de contrôle nationales.

En outre, l'ACC a décidé d'engager une action auprès du grand public, en élaborant une plaquette d'information diffusée, dans chacune des langues des Etats Schengen et en anglais, dans les postes consulaires et points d'entrée dans « l'espace Schengen », tels que les aéroports.

Une telle diffusion à grande échelle nécessite évidemment la coopération des pouvoirs publics. La plupart des Etats-membres ont parfaitement répondu aux v œux de l'ACC, les autorités françaises devant incessamment diffuser cette brochure, notamment dans les consulats.

EUROPOL

Comme tous les fichiers nationaux le sont dans chacun des Etats-membres de l'Union européenne, les fichiers d'Europol sont placés sous le contrôle d'une autorité de contrôle commune exclusivement composée de représentants des autorités nationales de contrôles des Etats-membres.

A ce jour, le système d'informations Europol qui doit être alimenté par les Etats-membres n'est pas mis en œuvre. Toutefois, plusieurs fichiers d'analyse sont en cours de constitution. L'autorité de contrôle commune est systématiquement informée de la création de tels fichiers et peut former toutes observations qu'elle estime nécessaires.

En outre, l'autorité de contrôle commune peut procéder à des visites sur place, d'initiatives ou à la demande de particuliers, pour vérifier les conditions de fonctionnement et de régularité des fichiers mis en œuvre.

Un droit d'accès reconnu

L'article 19 de la convention Europol précise clairement que « toute personne désirant exercer son droit d'accéder aux données la concernant, stockées à Europol, ou les faire vérifier peut, à cet effet, formuler gratuitement une demande dans tout Etat-membre de son choix à l'autorité nationale compétente qui saisit alors sans délai Europol et avise le requérant qu'Europol lui répondra directement ». Europol dispose alors d'un délai de trois mois à compter de la réception de la demande par l'autorité nationale compétente pour la traiter.

Le droit d'accès s'exerce donc obligatoirement par l'intermédiaire de l'une des autorités de contrôle nationales et selon la procédure prévue par le droit national. Le droit d'accès sera donc, au choix du requérant, soit un droit d'accès direct (tel

sera le cas par exemple s'il saisit l'autorité de contrôle allemande), soit un droit d'accès indirect (tel sera le cas, par exemple, s'il saisit la CNIL ou la Commission de la vie privée belge).

Europol procède aux vérifications en « étroite coordination avec les autorités nationales concernées », en France, la CNIL. En application du droit national, il sera notifié, en France, selon les termes mêmes de l'article 39 de la loi du 6 janvier 1978 que « les vérifications ont été faites ».

Mais Europol pouvant être considéré, en l'espèce, comme juge et partie, la convention Europol et le règlement intérieur de l'autorité commune ont aménagé des voies de recours contre les décisions d'Europol ou en cas de silence d'Europol à l'expiration d'un délai de trois mois courant à compter de la demande de droit d'accès.

L'aménagement de voies de recours

Ce droit de recours s'exerce devant le comité des recours, émanation « quasi-juridictionnelle » de l'autorité de contrôle commune.

Le comité des recours dispose de très importants pouvoirs. Ainsi, il peut à l'occasion de l'examen de l'affaire dont il est saisi, enquêter sur place auprès d'Europol, entendre à leur demande, les parties, des témoins et, d'initiative, s'il y a lieu des experts. La procédure est orale et publique, sauf motif tiré de la sécurité publique, de la protection de la vie privée d'une personne ou des spécificités de l'affaire. Si un Etat-membre ou Europol sollicite le huis clos, il peut être passé outre à cette demande à l'unanimité des représentants des autorités nationales de contrôle composant le comité des recours. Un procès-verbal reflétant les travaux du comité des recours est établi pour chaque affaire et transmis aux parties. La décision prise par le comité des recours est annoncée publiquement et communiquée aux parties.

Cette procédure, dont les modalités ont fait l'objet de nombreuses discussions entre les autorités indépendantes de contrôle, les gouvernements et les autorités d'Europol, a été définitivement arrêtée dans le règlement intérieur de l'ACC. Elle paraît, en l'état, offrir aux particuliers des garanties, de la nature de celles qui leur sont reconnues devant les juridictions nationales, pour des contentieux de cette nature.

3) VERS UNE APPROCHE HORIZONTALE ?

Une position de principe

« L'approche horizontale » vise à harmoniser les différentes règles de protection des données contenues dans les conventions conclues ou mises en œuvre dans le cadre du troisième pilier de l'Union européenne (Schengen, Europol, SID) et de créer une autorité de contrôle commune à l'ensemble des systèmes informatisés.

Cette question a fait l'objet d'une résolution des commissaires européens à la protection des données, lors de la réunion de Dublin des 23 et 24 avril 1998, qui affirme notamment que « l'efficacité de la protection [...] dépend dans une large

mesure tant du niveau d'harmonisation des règles de fond et de procédures que de la stricte coordination des recours et des garanties assurés par les différentes conventions ».

Enfin, elle fait l'objet de travaux au sein du « groupe horizontal » du Conseil européen. En particulier, une étude ayant pour objet de faire apparaître les différences entre les instruments du troisième pilier et d'en indiquer, dans la mesure du possible, les raisons (tenant par exemple aux différences d'architecture des systèmes informatisés), est en cours.

Un début de mise en œuvre

Sans aucun doute, la première étape de l'harmonisation consiste-t-elle à organiser les travaux des différentes autorités de contrôle commune de sorte que les représentants des autorités nationales qui les composent puissent disposer d'une vue d'ensemble. D'ores et déjà, les réunions de l'ACC Schengen et de l'ACC Europol se déroulent successivement au cours d'une même période.

La prochaine étape sera vraisemblablement la mise sur pied d'un secrétariat commun. Un projet de décision du Conseil instaurant un secrétariat unique pour les autorités de contrôle commune Schengen, Europol et SID (pour les aspects qui relèvent du volet intergouvernemental) est en cours de préparation.

Des limites

Sans doute, l'approche horizontale rencontre-t-elle deux limites.

La première tient à l'architecture des systèmes qui n'est pas la même d'un fichier à un autre. A cet égard, la référence à Europol ne paraît pas pouvoir servir de cadre général dans la mesure où les fichiers d'analyse d'Europol étant constitués au niveau européen ne peuvent pas être contrôlés par les autorités nationales, à la différence par exemple de ce qui se passe dans le cas de Schengen qui constitue une plate-forme jouant le rôle d'interface entre différentes bases nationales dont chacune peut être contrôlée par une autorité nationale.

La deuxième limite tient à la nécessité de ne pas éloigner le citoyen ou l'étranger résidant sur le territoire d'un Etat membre de son interlocuteur de proximité, c'est-à-dire, de l'autorité de contrôle nationale.

Ces limites expliquent sans doute la relative disparité des mécanismes de contrôle mis en œuvre. Elles ne sauraient cependant dissuader les personnes d'exercer leurs droits. Contrairement à ce qui a pu être dit ou écrit, aucun fichier de police européen ne fonctionne sans contrôle, et ce contrôle est, dans tous les cas, exercé par une autorité indépendante des gouvernements et des autorités (nationales ou européennes) de police. Gratuits, s'exerçant en France, par l'intermédiaire de la CNIL, ouvrant sur des voies de recours (les juridictions administratives françaises, s'agissant de Schengen, ou le comité des recours de l'autorité de contrôle commune Europol), ces droits doivent être exercés, si l'on souhaite parvenir à l'harmonisation des règles de fonctionnement des autorités de contrôle et celles des jurisprudences,

dans l'attente, le cas échéant, de la constitution d'une seule et même autorité de contrôle des fichiers européens de police.

B. Le contrôle des flux de données à l'intérieur de l'espace européen

La directive du 24 octobre 1995 constitue désormais un socle commun de protection des données personnelles dans l'espace européen. Elle détermine notamment des règles d'application du droit national et de coopération entre autorités nationales de contrôle. Ce texte, qui a été complété par d'autres directives sectorielles qui peuvent comporter des dispositions en matière de protection des données, a par ailleurs institué un groupe européen de protection des données dont l'influence devient un élément majeur de la protection des données personnelles dans l'Union européenne.

1) LA DIRECTIVE EUROPÉENNE DU 24 OCTOBRE 1995 ET LES AUTRES TEXTES APPLICABLES

Critère de détermination du droit national applicable

L'article premier de la directive précise clairement l'un des objectifs principaux de l'harmonisation des législations européennes : assurer la libre circulation des données dans l'espace européen en faisant interdiction aux Etats-membres de la restreindre ou de l'interdire au sein de l'Union européenne au prétexte d'un niveau insuffisant de protection. Ainsi, aucune distinction n'est plus établie selon que les données s'échangent entre des opérateurs situés sur le même territoire national ou entre les opérateurs situés sur le territoire de plusieurs Etats-membres. En un mot, il n'y a pas de « flux transfrontières de données » à l'intérieur de l'Union européenne. Cela ne signifie pas, bien entendu, que des données personnelles seraient moins protégées qu'auparavant puisque désormais tous les pays de l'Union européenne sont dotés d'une loi « informatique et libertés » et d'une autorité indépendante de contrôle et que ces législations s'harmonisent entre elles au fur et à mesure de la transposition de la directive dans les droits nationaux.

En outre, la directive détermine quelle est la loi nationale qui s'applique aux traitements des données à l'intérieur de l'Union européenne. Ainsi, l'article 4 de la directive prévoit que le droit national applicable est celui de l'Etat-membre sur le territoire duquel le responsable du traitement a son établissement. Conformément à la jurisprudence de la Cour européenne de justice, le considérant 19 de la directive précise que la notion d'établissement « suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable », sa forme juridique, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, important peu.

La directive précise que « si un même responsable du traitement est établi sur le territoire de plusieurs Etats membre, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ».

En outre, il résulte de l'article 17 de la directive qu'en cas de sous-traitance, le sous-traitant doit respecter les obligations prévues par la législation de l'Etat-membre sur le territoire duquel il est établi.

Enfin, le considérant 21 de la directive précise que « la directive ne préjuge pas des règles de territorialité applicables en matière de droit pénal ». Cela signifie que les règles particulières qui régissent en France la collecte de données sensibles ou le défaut de mentions légales d'information des personnes, qui sont pénalement sanctionnées, trouveront à s'appliquer même si le responsable du traitement est établi sur le territoire d'un autre Etat-membre.

Ces règles de détermination du droit national applicable et l'harmonisation des législations européennes tendent incontestablement à un renforcement du dispositif de protection qui existe en Europe. Bien sûr, les autorités européennes de protection des données seront amenées à coopérer, comme elles le font d'ailleurs depuis de nombreuses années, et la CNIL est de plus en plus fréquemment saisie par ses homologues européens lorsqu'un responsable de traitement mis en cause dans un autre Etat-membre est établi en France.

Les autres textes applicables

D'autres directives européennes, sectorielles, sont venues compléter le dispositif de protection, telle 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 ou la récente directive relative à certains aspects juridiques du commerce électronique. Aucune d'entre elles cependant ne déroge aux règles générales de protection des données personnelles posées par la directive du 24 octobre 1995 ni aux règles de détermination du droit national applicable en matière de protection de données personnelles.

2) LE GROUPE DIT « DE L'ARTICLE 29 »

L'article 29 de la directive du 24 octobre 1995 a institué un organe consultatif et indépendant, composé de représentants des autorités de contrôle de chaque Etat-membre. Ce groupe, dont la Commission européenne assure le secrétariat a pour mission d'examiner toute question portant sur la mise en œuvre des dispositions nationales de transposition de la directive, en vue de contribuer à leur harmonisation, de conseiller la Commission européenne sur toute mesure à prendre pour compléter les dispositions européennes en matière de protection des données personnelles, de donner un avis sur les codes de conduites élaborés au niveau communautaire et de donner à la Commission européenne un avis sur le niveau de protection assuré dans la Communauté et dans les pays tiers. En outre, le groupe peut, d'initiative, émettre des recommandations sur « toute question concernant la protection des personnes à l'égard des traitements de données à caractère personnel dans la Communauté ».

Ce groupe se réunit pratiquement une fois par mois à Bruxelles pour des sessions de travail en réunion plénière ou en sous groupes de travail, qui peuvent durer

plusieurs jours, ses avis sont diffusés sur le site Europa de la Commission européenne (http://www.europa.en.int/comm/dig15). Il rend publique un rapport annuel d'activité.

L'activité de ce groupe aura été particulièrement intense en 1999. Ainsi, le groupe a suivi de très près l'évolution du dialogue établi avec les Etats-Unis et a été amené à donner à quatre reprises son avis à la Commission européenne sur les diverses propositions faites par le Département du Commerce américain (voir infra). Il a procédé en outre à l'appréciation du niveau de protection assurée dans plusieurs pays tiers (5 avis), ainsi qu'à l'examen de plusieurs questions relatives à la protection des données personnelles sur internet (3 avis et recommandations). Par ailleurs, le groupe a poursuivi ses contacts avec les professionnels de plusieurs secteurs concernant l'élaboration de codes de conduite européens.

Appréciation du niveau de protection assuré dans les pays tiers

Le groupe est chargé de donner à la Commission européenne des avis sur le niveau de protection assuré par des pays-tiers. Il s'agit alors d'apprécier, au cas par cas, si les législations nationales ou les mesures prises par ces pays offrent un niveau de protection satisfaisant.

S'appuyant sur une méthode d'évaluation définie et rendue publique dans un avis du 24 juillet 1998, le groupe a été en mesure de donner un avis favorable à la Suisse et à la Hongrie. A la date de rédaction du présent rapport, la Commission européenne n'avait pas pris la décision visant à la reconnaissance du niveau adéquat de protection dans ces deux Etats (art. 25 de la directive).

La Norvège et l'Islande, liées à l'Union européenne par l'Accord Economique Européen, doivent transposer dans leur droit interne la directive 95/46, sauf notification contraire de la part de ces Etats à la Commission européenne non intervenue à ce jour. A l'issue de ce processus, ces Etats devraient être considérés comme assurant une protection adéquate.

C'est au titre de cette mission particulière, que le groupe a eu à examiner les propositions américaines de « safe harbor » (cf infra).

Enfin, le groupe a examiné plusieurs versions du projet de clauses types de contrat « protection des données » élaborées par la Chambre de Commerce Internationale destinées à offrir des garanties suffisantes de protection lorsque l'entreprise destinataire des données est établie dans un pays tiers qui n'assure pas un niveau de protection adéquat (article 26-2 de la directive). Cet exercice n'avait pas encore abouti à la date de clôture de ce rapport annuel. En effet, le groupe a estimé en particulier que la disparité des situations entre la sous-traitance, la gestion du personnel dans les multinationales ou le domaine commercial devait conduire, pour tenir compte d'exigences particulières selon ces différents domaines, à des développements spécifiques et non à l'établissement d'un modèle de contrat unique.

Internet

Le groupe a choisi de traiter en 1999 les questions qui lui paraissaient présenter un intérêt stratégique. Les avis et recommandations du groupe sont préparés par un sous groupe de travail comprenant des experts des différentes autorités dont les compétences sont à la fois juridiques et techniques.

• Avis sur les « traitements invisibles »

Le groupe a adopté le 3 février 1999 une recommandation concernant le traitement de données susceptibles d'être générées par les matériels et logiciels internet de manière invisible pour les intenautes qui les utilisent (identifiants de processeurs, cookies, liens hypertextes invisibles etc.).

Cette recommandation, dont le texte est annexé au présent rapport, s'adresse à l'industrie et rappelle qu'en application des principes de base de la protection des données de tels traitements devraient en réalité être conçus de manière à ce que les internautes en soient informés et puissent décider du moment et de la nature des informations à communiquer. Enfin, cette recommandation vise à inciter les industriels et éditeurs de logiciels à livrer les produits qu'ils commercialisent dans l'état de fonctionnement qui assure le niveau de protection maximum (par exemple n'acceptant pas l'enregistrement d'un cookie) accompagnés des explications nécessaires pour la mise en œuvre des autres options.

• Avis sur la durée de conservation des données de connexion

Dans le contexte des travaux conduits par le G8 sur la cyber-criminalité et des questions qui se posent dans tous les Etats membres sur la légitimité et la durée de la conservation des données de connexions à internet, le groupe a adopté le 7 septembre 1999 une recommandation annexée au présent rapport « sur la préservation des données de trafic par les fournisseurs de service Internet pour le respect du droit ».

Dans cette recommandation, le groupe précise que les données de connexion à internet sont des données à caractère personnel au sens de la directive 95/46 et reconnaît que ces données peuvent être conservées légitimement dans un souci de sécurité publique au-delà de la durée que justifierait la seule finalité de leur traitement (la connexion à internet). Le groupe ne prend pas parti sur une durée maximale de conservation, les pratiques étant variables d'un Etat membre à un autre, mais constate que ceux des pays qui ont fixé cette durée de conservation à trois mois ne paraissent pas rencontrer de problème particulier.

• Avis sur les données publiques

Le groupe a adopté un troisième avis le 3 mai 99 dans le contexte de la consultation publique organisée par la Commission européenne sur la base d'un livre vert sur l'accès à l'information émanant du secteur public dans le contexte de la société de l'information.

Cet avis, annexé au rapport, s'appuie sur de nombreux travaux conduits au plan national sur cet important sujet au cours des dernières années par les autorités de protection des données. Il montre à l'aide d'exemples, d'une part comment les

changements d'échelle tant quantitatifs que géographiques liés à l'utilisation des technologies de l'information doivent conduire à la prise de précautions particulières lorsque l'on facilite l'accès aux registres publics par des moyens électroniques. Ces précautions conduisent souvent, selon le cas et les risques particuliers encourus pour les personnes concernées, soit à ne pas publier les informations, soit à les rendre anonymes, soit à limiter les informations publiées. Il montre également comment il est possible d'utiliser la flexibilité des technologies de l'information pour limiter les risques encourus et en particulier pour contenir la consultation des données dans les limites des finalités poursuivies.

- Avis sur la prospection commerciale et le « spam »

Dans le cadre de l'adoption de la directive sur certains aspects du commerce électronique, le groupe adopté le 3 février 2000 un avis portant en particulier sur la prospection commerciale par e mail et le « spam » qui reprend l'ensemble des préconisations de la CNIL (cf. chapitre 3 et annexe 11).

Autres travaux

Le groupe a poursuivi les contacts établis avec la Fédération Européenne du Marketing Direct (FEDMA) à propos d'un projet de code de conduite européen ainsi qu'avec IATA sur la modification de sa recommandation internationale sur la protection des données destinée à tenir compte de la directive européenne dans le secteur du transport aérien.

Enfin, le groupe a engagé des travaux en vue d'établir les procédures communes pour la mise en œuvre de la coopération entre autorités nationales prévue à l'article 26-6 de la directive 95/46 en matière de traitement des plaintes visant des traitements de données impliquant plusieurs Etats membres.

C. Le contrôle des fichiers des institutions européennes

Le traité d'Amsterdam a introduit un article 213 b dans le traité destiné à assurer l'application de la réglementation européenne en matière de protection des données aux traitements de données à caractère personnel mis en œuvre dans les institutions européennes. A cette fin, la Commission a présenté en 1999 un projet de règlement ¨¨de l'adoption de ce texte, une nouvelle autorité indépendante sera désignée au plan européen qui sera également représentée au sein du groupe dit « de l'article 29 ».

Ce socle commun de garanties, qui est d'ailleurs appelé à être consacré dans la future « Charte des droits fondamentaux », est essentiel et constitue une véritable « force de frappe européenne » au service des droits de l'Homme dans le monde, ce dont témoigne, notamment, le cours des discussions engagées entre l'Europe et les Etats-Unis en matière de flux transfrontières de données.

II. LES DISCUSSIONS BILATÉRALES EUROPE — ÉTATS-UNIS SUR LE « SAFE-HABOR »

L'article 25.1 de la directive du 24 octrobre 1995 pose le principe du niveau de protection « adéquat » : un transfert de données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement après leur transfert ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat.

Cet article définit, ensuite, la manière dont s'apprécie le caractère adéquat du niveau de protection offert (art. 25.2), prévoit que les Etats-membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat (art. 25.3) et établit des règles destinées à résoudre les divergences de vue sur ce point entre les Etats-membres et la Commission (art. 25.4, 5 et 6). Il en résulte que lorsque la Commission constate qu'un pays tiers n'assure pas un niveau de protection adéquat, les Etats-membres doivent se conformer à sa décision et prendre « les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause ».

L'article 25-6 de la directive prévoit que la Commission européenne peut également constater, après avis du groupe de l'article 29, et d'un groupe composé des représentants des Etats-membres (dit « groupe de l'article 31 ») qu'un pays tiers assure un niveau de protection adéquat en raison de sa législation interne ou de ses engagements internationaux. Dans ce cas, les Etats-membres doivent prendre les mesures nécessaires pour se conformer à la décision de la Commission.

C'est sur le fondement de cet article que des discussions ont été entreprises il y a deux ans entre l'Europe et les Etats-Unis sur un modèle original d'engagement international de la part de ce pays tiers et qui répond au nom de « Safe harbor » que l'on pourrait traduire par l'expression « havre de sécurité ».

Le groupe de l'article 29 a suivi pas à pas l'état d'avancement de ces discussions auxquelles il a directement été associé par la Commission européenne. Il a rendu un important avis le 4 novembre 1999, encore très réservé sur le caractère suffisant, au regard des exigences de la directive européenne, des propositions américaines. Les mois qui ont suivi ont cependant permis de réaliser de nets progrès dans les discussions.

A la date de rédaction du présent rapport, l'accord de « Safe harbor » n'est pas définitivement conclu. Compte tenu, toutefois, de l'originalité du dispositif proposé, de son importance et du travail de conviction et de négociation qui a été accompli en direction des autorités américaines, tout particulièrement par le groupe de l'article 29, il apparaît indispensable d'en présenter les grandes lignes et les enjeux ainsi que les observations qu'il peut appeler.

A. Le principe : une adhésion volontaire des entreprises américaines à un corps de principes de protection des données

Les entreprises américaines qui le souhaitent pourraient adhérer à un corps de principes de protection de la vie privée considérés par l'Union européenne comme assurant un niveau de protection adéquat autorisant les flux transfrontières de données sans que les Etats-membres ou les autorités nationales de contrôle ne puissent s'y opposer.

Au titre de ces principes qui reprennent pour l'essentiel ceux qui sont énumérés par la directive européenne, figurent notamment les engagements suivants.

Les entreprises adhérentes s'engageraient à informer les personnes de la finalité du traitement et des usages possibles des données collectées, lors de la collecte des données ou « dès que possible » après la collecte.

Les entreprises s'engageraient à offrir aux personnes concernées la faculté de s'opposer à un usage des données qui serait incompatible avec les finalités ayant présidé à la collecte et le droit de s'opposer à la communication des données à des tiers pour un autre usage que la finalité initiale.

Les entreprises s'engageraient à ne collecter les données sensibles qu'avec le consentement exprès des personnes concernées.

Les entreprises reconnaîtraient le droit d'accès des personnes concernées, s'engageraient, sous les conditions précédemment définies, à ne céder des données personnelles qu'à d'autres entreprises adhérentes au « safe harbor » ou reconnues comme offrant un niveau de protection adéquat.

Enfin, les entreprises devraient s'engager à assurer la sécurité du traitement et l'intégrité des données.

Ces grands principes sont ensuite déclinés sous la forme de « questions-réponses » sur des problèmes d'application concrets correspondant aux questions les plus fréquemment posées par les entreprises américaines (FAQ).

Il est incontestable que de grands progrès ont été accomplis au cours des discussions entre l'Europe et la partie américaine qui ont considérablement rapproché les points de vue, et les concepts fondamentaux, tant dans leur définition (données à caractère personnel par exemple) que dans l'énoncé des principes.

B. Le fondement juridique de l'éventuel accord

Il s'agirait d'une décision de la Commission européenne prise sur le fondement de l'article 25-6 de la directive de 1995 et reconnaissant le caractère adéquat des principes figurant dans le « Safe harbor » et les documents annexés (les FAQ).

En outre, un échange de lettres entre le représentant de la partie américaine, sous-secrétaire d'Etat au commerce, et le directeur général de la Commission

européenne, accompagnerait cet accord. Il résulterait de cet échange de lettres qu'un bilan d'application serait fait au début 2003.

C. La portée de l'accord

Les gouvernements des pays européens et les autorités nationales de protection des données se sont tout particulièrement attachés à ce que les entreprises américaines comprennent que les principes du « safe harbor » ne se substituaient pas aux règles prévues par la directive en matière d'application du droit national, s'agissant tout particulièrement des conditions dans lesquelles des données personnelles peuvent être collectées en Europe.

Il convient à cet égard de rappeler que selon l'article 4.1-c de la directive, le droit national de protection des données doit être appliqué par tout responsable de traitement qui, n'étant pas établi sur le territoire de la Communauté, recourt à des moyens automatisés ou non situés sur le territoire d'un Etat-membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit. Ainsi, les entreprises américaines qui souhaitent collecter des données en Europe, doivent respecter le droit national de chaque Etat-membre. Le « safe harbor » ne peut donc en aucun cas « dégrader » les garanties offertes en Europe par les législations nationales. Il a pour objet et pour effet de prolonger ces garanties lorsque les données collectées en Europe sont cédées ou transmises à des entreprises établies sur le territoire des Etats-Unis.

Sur ce point également, des garanties ont été apportées au cours des discussions entre l'Europe et les Etats-Unis et les projets d'échange de lettres comme plusieurs FAQ précisent que le droit national européen sera en tout état de cause appliqué par les entreprises américaines qui collectent des données sur le territoire européen.

D. Les engagements pris par les américains pour assurer l'effectivité du « safe harbor »

L'un des problèmes essentiels des discussions transatlantiques tient aux modalités de mise en œuvre et de vérification des engagements pris par les entreprises américaines et de résolutions des litiges pouvant survenir.

A la date de rédaction du présent rapport, les garanties apportées par la partie américaine étaient les suivantes.

La procédure d'adhésion :

L'entreprise souhaitant adhérer au « safe harbor » doit se faire connaître auprès du ministère américain du commerce ou d'une personne qui serait désignée par ce ministère. Elle remet alors une lettre signée précisant son nom et ses coordonnées, décrivant ses activités et les dispositions prises en matière de protection des données. Elle doit en outre désigner un délégué à la protection des données, chargé en particulier de répondre aux demandes de droit d'accès et aux plaintes, préciser l'instance

réglementaire, dont l'entreprise dépend, chargée d'instruire d'éventuels recours et la nature du programme de protection des données auquel elle participe.

Le ministère américain tiendra la liste des entreprises adhérentes à jour et la rendra publique.

Toutefois, cette déclaration d'une entreprise pourra donner lieu à des poursuites devant la Commission fédérale du commerce (FTC) ou devant toute autre instance administrative compétente.

Procédure de contrôle de la sincérité de l'adhésion :

Toute entreprise adhérant au « safe harbor » doit procéder à un audit annuel des mesures prises en matière de protection des données personnelles. Un compte-rendu écrit doit en être établi et tenu à la disposition des consommateurs qui en feront la demande ou, dans le cadre de l'instruction d'une plainte, à l'organisme indépendant ou à l'agence compétente pouvant en être saisie.

Mécanisme de résolution des litiges :

Toutes les entreprises adhérant au « safe harbor » doivent dépendre d'une instance indépendante susceptible d'examiner les plaintes de particuliers. Cette obligation peut cependant être satisfaite par l'adhésion de l'entreprise à un programme d'autorégulation mais à la condition que la méconnaissance de ce programme puisse être sanctionné par des décisions ayant force exécutoire.

Les recours exercés contre les entreprises doivent pouvoir aboutir à des sanctions effectives, le cas échéant, assorties d'une publication.

La méconnaissance persistance des principes pourra conduire le ministère du commerce à exclure une entreprise adhérente de la liste du « safe harbor ».

Engagement à coopérer avec les autorités européennes de protection des données :

Il s'agit d'une option ouverte aux entreprises américaines qui consiste pour elles à s'engager à suivre tous les avis qui seront données par les autorités européennes de protection des données, en pratique une émanation du groupe de l'article 29. Cette instance particulière pourrait alors être saisie directement par des particuliers d'une plainte formée contre une entreprise américaine.

Tel était, dans ces grandes lignes, le dispositif du « safe harbor » à la date de rédaction du présent rapport.

Le 16 mai 2000, le groupe de l'article 29 a rendu un avis sur le « safe harbor » publié en annexe. Le groupe enregistre les progrès sensibles visant à améliorer la protection des données à caractère personnel qui ont été réalisés au cours des deux dernières années, mais relève encore certaines imperfections en mettant plus particulièrement l'accent sur la nécessité de prévoir l'existence d'une instance indépendante pouvant être saisie, aux Etats-Unis, par toute personne concernée par un traitement. A cet égard, il souhaiterait que le champ d'application du « safe harbor »

soit parfaitement défini, tant en ce qui concerne le droit applicable que les compétences des organismes publics pouvant apprécier le respect des engagements des entreprises américaines en matière de protection des données personnelles. Enfin, s'agissant tout particulièrement des sites internet, et reprenant la proposition de la délégation française, le groupe invite la Commission européenne à engager en priorité les travaux nécessaires à l'établissement d'un système de labellisation européenne des sites internet sur la base d'un référentiel d'évaluation commun à l'ensemble des Etats-membres.

Quelle que soit l'issue de ces longues discussions, il convient de souligner que les gouvernements des Etats-membres, la Commission européenne, la CNIL et ses homologues européens ont, jusqu'à présent, agi de concert dans les discussions menées entre l'Europe et les Etats-Unis, avec en main un seul « carnet de route » : la directive européenne du 24 octobre 1995 qui se révèle être un puissant levier de la protection des données personnelles dans le monde autour d'une commune conviction européenne.

ANNEXES

Composition de la Commission au 31 mai 2000

Président : **Michel GENTOT**, président de section au Conseil d'Etat,

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'Etat

André BOHL, sénateur de Moselle, maire de Creutzwald

Noël CHAHID-NOURAÏ, conseiller d'Etat

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'Etat honoraire

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social

Alex TÜRK, 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

Composition de la Commission au 31 décembre 1999

Président : **Michel GENTOT**, président de section au Conseil d'Etat,

Vice-président délégué : **Hubert BOUCHET**, membre du Conseil économique et social, secrétaire général de l'Union des Cadres et Ingénieurs Force Ouvrière

Vice-président : **Raymond FORNI**, vice-président de l'Assemblée Nationale, député du Territoire-de-Belfort, maire de Delle

Commissaires :

Cécile ALVERGNAT, directrice générale de l'Echangeur

Maurice BENASSAYAG, conseiller d'Etat

Noël CHAHID-NOURAÏ, conseiller d'Etat

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Gérard GOUZES, député du Lot-et-Garonne, maire de Marmande

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'Etat honoraire

Jean-Marie POIRIER, conseiller d'Etat honoraire, sénateur du Val de Marne, maire de Sucy-en-Brie

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social

Alex TÜRK, sénateur du Nord

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

Répartition des secteurs d'activité

Hubert BOUCHET, vice-président délégué : emploi, recrutement, formation, élections professionnelles

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)

Noël CHAHID-NOURAÏ : trésor public, fiscalité, cadastre, publicité foncière, douanes, répression des fraudes, comptabilité publique, droit d'accès indirect

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

Gérard GOUZES : justice (autorité judiciaire, justice administrative, professions judiciaires), autorités administratives indépendantes, archives nationales

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

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 (GERI et groupe dit « de Berlin »), 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 TÜRK : 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

Organigramme des services au 31 mai 2000

Président : **Michel GENTOT**

Secrétaire général chargé des affaires juridiques : **Joël BOYER,** magistrat

Secrétariat de la Présidence :
Odile BOURRE, chef du secrétariat
Véronique BREMOND
Evelyne LE CAM

Direction de l'administration, des finances et de la communication

Directeur : **Thierry JARLET**, chargé de mission

Secrétariat :
Brigitte BARBARANT

SERVICE DE L'ADMINISTRATION ET DU PERSONNEL

Chef de service : **Marie-Thérèse BIASINI**, chargée de mission

Missions — Déplacements :
Brigitte SALHI

Standard téléphonique — accueil :
Marie-Christiane BENJAMIN
Monique GOURDELIER

Téléphonie — Télématique :
Sébastien BÉNARD,
Giuseppe GIARMANA

Courrier — Reprographie :
Sébastien BÉNARD
Giuseppe GIARMANA
Karim MANSOUR

Conducteurs :
Alain HOUDIN
Joël LEPAGE
Patrick MAHOUDEAU

Entretien :
Felisa RODRIGUEZ

CELLULE BUDGET ACHATS COMPTABILITÉ

Budget — Fonctionnement — Services intérieurs :
Jean-Claude BARACASSA, chargé de mission

Comptabilité — Paie — Vacations :
Liliane RAMBERT

SERVICE DE L'INFORMATION ET DE LA DOCUMENTATION

Chef de service : **Edmée MOREAU**, chargée de mission

Ingénierie documentaire — Webmaster :
Louis RAMIREZ, attaché

Documentation juridique — Relations avec le public :
Perrine CHEVILLON, attachée

Revue de presse — Information générale :
Hervé GUDIN, attaché

Rapport d'activité :
Edmée MOREAU, chargée de mission

Direction juridique

Secrétariat :
Marie-Paule FORTASSIN
Brigitte HUGER

SERVICE CHARGÉ DES LIBERTÉS PUBLIQUES, DE LA SANTÉ
ET DE LA PROTECTION SOCIALE

Chef de service : **Sophie VULLIET-TAVERNIER,** chargée de mission

Intérieur — Défense — Affaires Étrangères — Coopération européenne et internationale dans ce domaine — Police municipale :
Florence FOURETS, chargée de mission

Fiscalité — Douanes — Répression des fraudes — Coopération européenne et internationale dans ce domaine :
Olivier COUTOR, chargé de mission

Santé — Recherche :
Jeanne BOSSI, chargée de mission
Caroline PARROT, attachée

Sécurité sociale — Mutuelles :
Sandrine SARROCHE, attachée

Aide sociale — Allocations familiales — RMI :
Norbert FORT, attaché

Gestion des collectivités locales :

Norbert FORT, attaché

Bérengère MONEGIER DU SORBIER, chargée de mission

Justice — Libertés publiques — Archives :

Emilie PASSEMARD, attachée

Droit d'accès indirect :
Bérengère MONEGIER DU SORBIER, chargée de mission

Secrétariat:
Véronique FOUILLET
Brigitte HUGER
Eugénie MARQUES
Michèle SAISI

SERVICE CHARGÉ DE L'ÉCONOMIE, DE L'EMPLOI ET DE L'ÉDUCATION

Chef de service : **Sophie NERBONNE**, chargée de mission

Éducation — Insee — Sport — Culture — Tourisme :
Fatima HAMDI, chargée de mission

Banque — Crédit — Bourse — Assurance — Renseignement commercial :
Nathalie BETHENCOURT, attachée
Guillaume DELAFOSSE, attaché

Secteur commercial — Marketing :
Odile JAMI, attachée
Françoise PARGOUD, attachée

Équipement — Urbanisme — Immobilier — Logement :
Odile JAMI, attachée

Travail :
Sandrine MATHON, attachée
Nicole GUILLEUX, attachée

Transports — Industrie — Énergies :
Guillaume DELAFOSSE, attaché

Environnement — Agriculture :
Françoise PARGOUD, attachée

Secrétariat :
Barbara BAVOIL
Valérie GAUTHIER

MISSION CHARGÉE DES TÉLÉCOMMUNICATIONS, DES SERVICES EN LIGNE ET DES RELATIONS AVEC LES CORRESPONDANTS ÉTRANGERS

Chef de la mission : **Marie GEORGES**, chargée de mission

Patrick AMOUZOU, attaché

N...

Secrétariat :
Anna BENISTI

BUREAU DES REQUÊTES GÉNÉRALES

Responsable du bureau : **Clémentine VOISARD**, chargée de mission

Plaintes — Demandes de conseil et d'informations générales — Refus d'accès et de rectification — contentieux d'habitude (VPC…)
Véronique JENNEQUIN

Secrétariat :
Françoise BANQUY

Direction informatique

Directeur : **Roger NGÔ**, ingénieur informaticien

Secrétariat :
Anna BENISTI

INFORMATIQUE INTERNE

Projets et développements :
Gilbert BENICHOU, informaticien de haute technicité

Statistiques :
Michel MORFIN, chef d'exploitation

Gestion des fichiers de la Commission — Validation déclarations simplifiées :
Michel MORFIN, chef d'exploitation
Bernard LAUNOIS, analyste programmeur
Paulette CHIES

Saisie informatique des dossiers :
Paulette CHIES,
Christiane MARIE
Sébastien BÉNARD

Gestion du parc et assistance technique :
Michel MORFIN, chef d'exploitation
Bernard LAUNOIS, analyste programmeur

Téléphonie :
Bernard LAUNOIS, analyste programmeur

EXPERTISE ET CONTRÔLE — SÉCURITÉ DES SYSTÈMES D'INFORMATION

Gilbert BENICHOU, informaticien de haute technicité

Jean-Paul MACKER, chargé de mission

Organigramme des services au 31 décembre 1999

Président : **Michel GENTOT**

Secrétaire général chargé des affaires juridiques : **Joël BOYER,** magistrat

Secrétariat de la Présidence :
Odile BOURRE, Chef du secrétariat
Véronique BREMOND
Evelyne LE CAM

Direction de l'administration, des finances et de la communication

Directeur : **Thierry JARLET**, chargé de mission

Secrétariat :
Brigitte BARBARANT

SERVICE DE L'ADMINISTRATION ET DU PERSONNEL

Chef de service : **Marie-Thérèse BIASINI**, chargée de mission

Missions — Déplacements :
Brigitte SALHI

Téléphonie — Télématique :
Sébastien BÉNARD,
Giuseppe GIARMANA

Courrier — Reprographie :
Sébastien BÉNARD
Giuseppe GIARMANA
Karim MANSOUR

Conducteurs :
Alain HOUDIN
Joël LEPAGE
Patrick MAHOUDEAU

Standard téléphonique — accueil :
Marie-Christiane BENJAMIN
Monique GOURDELIER

Entretien :
Felisa RODRIGUEZ

CELLULE BUDGET ACHATS COMPTABILITÉ

Budget — Fonctionnement — Services intérieurs :
Jean-Claude BARACASSA, chargé de mission

Comptabilité — Paie — Vacations :
Liliane RAMBERT

SERVICE DE L'INFORMATION ET DE LA DOCUMENTATION

Chef de service : **Edmée MOREAU**, chargée de mission

Ingénierie documentaire — Webmaster :
Louis RAMIREZ, attaché

Documentation juridique — Relations avec le public :
Perrine CHEVILLON, attachée

Revue de presse — Information générale :
Hervé GUDIN, attaché

Rapport d'activité :
Edmée MOREAU, chargée de mission

Direction juridique

Secrétariat :
Marie-Paule FORTASSIN
Brigitte HUGER

SERVICE CHARGÉ DES LIBERTÉS PUBLIQUES, DE LA SANTÉ
ET DE LA PROTECTION SOCIALE

Chef de service : **Sophie VULLIET-TAVERNIER,** chargée de mission

Intérieur — Défense — Affaires Étrangères — Coopération européenne et internationale dans ce domaine — Police municipale :
Florence FOURETS, chargée de mission

Fiscalité — Douanes — Répression des fraudes — Coopération européenne et internationale dans ce domaine :
Olivier COUTOR, chargé de mission

Santé — Recherche :
Jeanne BOSSI, chargée de mission
Caroline PARROT, attachée

Sécurité sociale — Mutuelles :
Sandrine SARROCHE, attachée

Aide sociale — Allocations familiales — RMI :
Norbert FORT, attaché

Gestion des collectivités locales :
Norbert FORT, attaché

Bérengère MONEGIER DU SORBIER, attachée

Justice — Libertés publiques — Archives :
Emilie PASSEMARD, attachée

Droit d'accès indirect :
Bérengère MONEGIER DU SORBIER, attachée

Secrétariat:
Véronique FOUILLET
Brigitte HUGER
Eugénie MARQUES
Michèle SAISI

SERVICE CHARGÉ DE L'ÉCONOMIE, DE L'EMPLOI ET DE L'ÉDUCATION

Chef de service : **Sophie NERBONNE**, chargée de mission

Éducation — Insee — Sport — Culture — Tourisme :
Fatima HAMDI, chargée de mission

Banque — Crédit — Bourse — Assurance — Renseignement commercial :
Laurent CARON, attaché
Guillaume DELAFOSSE, attaché

Secteur commercial — Marketing :
Odile JAMI, attachée
Françoise PARGOUD, attachée

Équipement — Urbanisme — Immobilier — Logement :
Odile JAMI, attachée

Travail :
Sandrine MATHON, attachée
Nicole GUILLEUX, attachée

Transports — Industrie — Énergies :
Guillaume DELAFOSSE, attaché

Environnement — Agriculture :
Françoise PARGOUD, attachée

Secrétariat :
Barbara BAVOIL
Valérie GAUTIER

MISSION CHARGÉE DES TÉLÉCOMMUNICATIONS, DES SERVICES EN LIGNE ET DES RELATIONS AVEC LES CORRESPONDANTS ÉTRANGERS

Chef de la mission : **Marie GEORGES**, chargée de mission

Étienne DROUARD, attaché

Secrétariat :
Anna BENISTI

BUREAU DES REQUÊTES GÉNÉRALES

Responsable du bureau : **Clémentine VOISARD**, attachée

Plaintes — Demandes de conseil et d'informations générales — Refus d'accès et de rectification — contentieux d'habitude (VPC…)
Véronique JENNEQUIN

Secrétariat :
Françoise BANQUY

Direction informatique

Directeur : **Roger NGÔ**, ingénieur informaticien

Secrétariat :
Anna BENISTI

INFORMATIQUE INTERNE

Projets et développements :
Gilbert BENICHOU, informaticien de haute technicité

Statistiques :
Michel MORFIN, chef d'exploitation

Gestion des fichiers de la Commission — Validation déclarations simplifiées :
Michel MORFIN, chef d'exploitation
Bernard LAUNOIS, analyste programmeur
Paulette CHIES

Saisie informatique des dossiers :
Paulette CHIES,
Christiane MARIE
Sébastien BÉNARD

Gestion du parc et assistance technique :
Michel MORFIN, chef d'exploitation
Bernard LAUNOIS, analyste programmeur

Téléphonie :
Bernard LAUNOIS, analyste programmeur

EXPERTISE ET CONTRÔLE — SÉCURITÉ DES SYSTÈMES D'INFORMATION

Gilbert BENICHOU, informaticien de haute technicité

Jean-Paul MACKER, chargé de mission

Loi n° 78-17 du 6 janvier 1978 [1] relative à l'informatique, aux fichiers et aux libertés

L'Assemblée nationale et le Sénat ont adopté.

Le Président de la République promulgue la loi dont la teneur suit :

Chapitre I — Principes et définitions

Article 1er

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Article 3

Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.

Article 4

Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale.

Article 5

Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives.

1 Journal officiel du 7 janvier 1978 et rectificatif au JO du 25 janvier 1978, modifiée par la loi n° 88-227 du 11 mars 1988, article 13 relative à la transparence financière de la vie politique (JO du 12 mars 1988), la loi n° 92-1336 du 16 décembre 1992 (JO du 23 décembre 1992), la loi n° 94-548 du 1er juillet 1994 (JO du 2 juillet 1994), la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle, art. 41 (JO du 28 juillet 1999) et la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations (JO du 13 avril 2000).

Chapitre II — La Commission nationale de l'informatique et des libertés

Article 6

Une Commission nationale de l'informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique aux traitements des informations nominatives. La commission dispose à cet effet d'un pouvoir réglementaire, dans les cas prévus par la présente loi.

Article 7

Les crédits nécessaires a la commission nationale pour l'accomplissement de sa mission sont inscrits au budget du ministère de la Justice. Les dispositions de la loi du 10 août 1922 relative au contrôle financier ne sont pas applicables à leur gestion. Les comptes de la commission sont présentés au contrôle de la Cour des comptes.

Toutefois, les frais entraînés par l'accomplissement de certaines des formalités visées aux articles 15, 16, 17 et 24 de la présente loi peuvent donner lieu à la perception des redevances.

Article 8

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante.

Elle est composée de dix-sept membres nommés pour cinq ans ou pour la durée de leur mandat :
— deux députés et deux sénateurs élus, respectivement par l'Assemblée nationale et par le Sénat ;
— deux membres du Conseil économique et social, élus par cette assemblée ;
— deux membres ou anciens membres du Conseil d'État, dont l'un d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'État ;
— deux membres ou anciens membres de la Cour de cassation, dont l'un d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;
— deux membres ou anciens membres de la Cour des comptes, dont l'un d'un grade au moins égal à celui de conseiller-maître, élus par l'assemblée générale de la Cour des comptes ;
— deux personnes qualifiées pour leur connaissance des applications de l'informatique, nommées par décret sur proposition respectivement du président de l'Assemblée nationale et du président du Sénat ;
— trois personnalités désignées en raison de leur autorité et de leur compétence par décret en conseil des ministres.

La commission élit en son sein, pour cinq ans, un président et deux vice-présidents.

La commission établit son règlement intérieur.

En cas de partage des voix, celle du président est prépondérante.

Si, en cours de mandat, le président ou un membre de la commission cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir.

La qualité de membre de la commission est incompatible :
— avec celle de membre du Gouvernement ;

— avec l'exercice de fonctions ou la détention de participation dans les entreprises concourant à la fabrication de matériel utilisé en informatique ou en télécommunication ou à la fourniture de services en informatique ou en télécommunication.

La commission apprécie dans chaque cas les incompatibilités qu'elle peut opposer à ses membres.

Sauf démission, il ne peut être mis fin aux fonctions de membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit.

Article 9

Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission.

Il peut, dans les dix jours d'une délibération, provoquer une seconde délibération.

Article 10

La commission dispose de services qui sont dirigés par le président ou, sur délégation, par un vice-président, et placés sous son autorité.

La commission peut charger le président ou le vice-président délégué d'exercer ses attributions en ce qui concerne l'application des articles 16, 17 et 21 (4°, 5° et 6°), ainsi que des articles 40-13 et 40-14 (Loi n° 99-641 du 27 juillet 1999, art. 41).

Les agents de la commission nationale sont nommés par le président ou le vice-président délégué.

Article 11

La commission peut demander aux premiers présidents de cour d'appel ou aux présidents de tribunaux administratifs de déléguer un magistrat de leur ressort, éventuellement assisté d'experts, pour des missions d'investigation et de contrôle effectuées sous sa direction.

Article 12

Les membres et les agents de la commission sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues (Loi n° 92-1336 du 16 décembre 1992, art. 256) « à l'article 413-10 du code pénal » et, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel prévu ci-après, (Loi n° 92-1336 du 16 décembre 1992, art. 333) « aux articles 226-13 et 226-14 » du code pénal.

Article 13

Dans l'exercice de leurs attributions, les membres de la Commission nationale de l'informatique et des libertés ne reçoivent d'instruction d'aucune autorité.

Les informaticiens appelés, soit à donner les renseignements à la commission, soit à témoigner devant elle, sont déliés en tant que de besoin de leur obligation de discrétion.

Chapitre III — Formalités préalables à la mise en œuvre des traitements automatisés

Article 14

La Commission nationale de l'informatique et des libertés veille à ce que les traitements automatisés, publics ou privés d'informations nominatives, soient effectués conformément aux dispositions de la présente loi.

Article 15

Hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés.

Si l'avis de la commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État ou s'agissant d'une collectivité territoriale, en vertu d'une décision de son organe délibérant approuvée par décret pris sur avis conforme du Conseil d'État.

Si, au terme d'un délai de deux mois renouvelable une seule fois sur décision du président, l'avis de la commission n'est pas notifié, il est réputé favorable.

Article 16

Les traitements automatisés d'informations nominatives effectués pour le compte de personnes autres que celles qui sont soumises aux dispositions de l'article 15 doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

Cette déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Dès qu'il a reçu le récépissé délivré sans délai par la commission, le demandeur peut mettre en œuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités.

Article 17

Pour les catégories les plus courantes de traitements à caractère public ou privé, qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie des normes simplifiées inspirées des caractéristiques mentionnées à l'article 19.

Pour les traitements répondant à ces normes, seule une déclaration simplifiée de conformité à l'une de ces normes est déposée auprès de la commission. Sauf décision particulière de celle-ci, le récépissé de déclaration est délivré sans délai. Dès réception de ce récépissé, le demandeur peut mettre en œuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités.

Article 18

L'utilisation du répertoire national d'identification des personnes physiques en vue d'effectuer des traitements nominatifs est autorisé par décret en Conseil d'État pris après avis de la commission.

Article 19

La demande d'avis ou la déclaration doit préciser :

— la personne qui présente la demande et celle qui a pouvoir de décider la création du traitement ou, si elle réside à l'étranger, son représentant en France ;

— les caractéristiques, la finalité et, s'il y a lieu, la dénomination du traitement ;
— le service ou les services chargés de mettre en œuvre celui-ci ;
— le service auprès duquel s'exerce le droit d'accès défini au chapitre V ci-dessous, ainsi que les mesures prises pour faciliter l'exercice de ce droit ;
— les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées ;
— les informations nominatives traitées, leur origine et la durée de leur conservation ainsi que leurs destinataires ou catégories de destinataires habilités à recevoir communication de ces informations ;
— les rapprochements, interconnexions ou toute autre forme de mise en relation de ces informations ainsi que leur cession à des tiers ;
— les dispositions prises pour assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi ;
— si le traitement est destiné à l'expédition d'informations nominatives entre le territoire français et l'étranger, sous quelque forme que ce soit, y compris lorsqu'il est l'objet d'opérations partiellement effectuées sur le territoire français à partir d'opérations antérieurement réalisées hors de France.

Toute modification aux mentions énumérées ci-dessus, ou toute suppression de traitement, est portée à la connaissance de la commission.

Peuvent ne pas comporter certaines des mentions énumérées ci-dessus les demandes d'avis relatives aux traitements automatisés d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique.

Article 20

L'acte réglementaire prévu pour les traitements régis par l'article 15 ci-dessus précise notamment :
— la dénomination et la finalité du traitement ;
— le service auprès duquel s'exerce le droit d'accès défini au chapitre V ci-dessous ;
— les catégories d'informations nominatives enregistrées ainsi que les destinataires ou catégories de destinataires habilités à recevoir communication de ces informations.

Des décrets en Conseil d'État peuvent disposer que les actes réglementaires relatifs à certains traitements intéressant la sûreté de l'État, la défense et la sécurité publique ne seront pas publiés.

Article 21

Pour l'exercice de sa mission de contrôle, la commission :

1°) Prend des décisions individuelles ou réglementaires dans les cas prévus par la présente loi ;

2°) Peut, par décision particulière, charger un ou plusieurs de ses membres ou de ses agents, assistés, le cas échéant, d'experts, de procéder, à l'égard de tout traitement, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission ;

3°) Édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ; en cas de circonstances exceptionnelles, elle peut prescrire des mesures de sécurité pouvant aller jusqu'à la destruction des supports d'informations ;

4°) 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 ;

5°) Veille à ce que les modalités de mise en œuvre du droit d'accès et de rectification indiquées dans les actes et déclarations prévus aux articles 15 et 16 n'entravent pas le libre exercice de ce droit ;

6°) Reçoit les réclamations, pétitions et plaintes ;

7°) Se tient informée des activités industrielles et de services qui concourent à la mise en œuvre de l'informatique.

Les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de fichiers nominatifs ne peuvent s'opposer à l'action de la commission ou de ses membres pour quelque motif que ce soit et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche.

Article 22

La commission met à la disposition du public la liste des traitements, qui précise pour chacun d'eux :
— la loi ou l'acte réglementaire décidant de sa création ou la date de sa déclaration ;
— sa dénomination et sa finalité ;
— le service auprès duquel est exercé le droit prévu au chapitre V ci-dessous ;
— les catégories d'informations nominatives enregistrées ainsi que les destinataires ou catégories de destinataires habilités à recevoir communication de ces informations.

Sont tenus à la disposition du public, dans les conditions fixées par décret, les décisions, avis ou recommandations de la commission dont la connaissance est utile à l'application ou à l'interprétation de la présente loi.

Article 23

La commission présente chaque année au Président de la République et au Parlement un rapport rendant compte de l'exécution de sa mission. Ce rapport est publié.

Ce rapport décrira notamment les procédures et méthodes de travail suivies par la commission et contiendra en annexe toutes informations sur l'organisation de la commission et de ses services propres à faciliter les relations du public avec celle-ci.

Article 24

Sur proposition ou après avis de la commission, la transmission entre le territoire français et l'étranger, sous quelque forme que ce soit, d'informations nominatives faisant l'objet de traitements automatisés régis par l'article 16 ci-dessus peut être soumise à autorisation préalable ou réglementée selon des modalités fixées par décret en Conseil d'État en vue d'assurer le respect des principes posés par la présente loi.

Chapitre IV — Collecte, enregistrement et conservation des informations nominatives

Article 25

La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite.

Article 26

Toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement.

Ce droit ne s'applique pas aux traitements limitativement désignés dans l'acte réglementaire prévu à l'article 15.

Article 27

Les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées :
— du caractère obligatoire ou facultatif des réponses ;
— des conséquences à leur égard d'un défaut de réponse ;
— des personnes physiques ou morales destinataires des informations ;
— de l'existence d'un droit d'accès et de rectification.

Lorsque de telles informations sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces prescriptions.

Ces dispositions ne s'appliquent pas à la collecte des informations nécessaires à la constatation des infractions.

Article 28

Sauf dispositions législatives contraires, les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration, à moins que leur conservation ne soit autorisée par la commission.

Article 28

(Modifié par la loi n° 2000-321 du 12 avril 2000, article 5, 1°)

I. — Au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou traitées, les informations ne peuvent être conservées sous une forme nominative qu'en vue de leur traitement à des fins historiques, statistiques ou scientifiques. Le choix des informations qui seront ainsi conservées est opéré dans les conditions prévues à l'article 4-1 de la loi no 79-18 du 3 janvier 1979 sur les archives.

II. — Les informations ainsi conservées, autres que celles visées à l'article 31, ne peuvent faire l'objet d'un traitement à d'autres fins qu'à des fins historiques, statistiques ou scientifiques, à moins que ce traitement n'ait reçu l'accord exprès des intéressés ou ne soit autorisé par la commission dans l'intérêt des personnes concernées. Lorsque ces informations comportent des données mentionnées à l'article 31, un tel traitement ne peut être mis en œuvre, à moins qu'il n'ait reçu l'accord exprès des intéressés, ou qu'il n'ait été autorisé, pour des motifs d'intérêt public et dans l'intérêt des personnes concernées, par décret en Conseil d'Etat sur proposition ou avis conforme de la commission.

Article 29

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.

Article 29-1

(Inséré par la loi n° 2000-321 du 12 avril 2000, article 5, 2°)

Les dispositions de la présente loi ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre Ier de la loi no 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal et des dispositions du titre II de la loi no 79-18 du 3 janvier 1979 précitée.

En conséquence, ne peut être regardé comme un tiers non autorisé au sens de l'article 29 le titulaire d'un droit d'accès aux documents administratifs ou aux archives publiques exercé conformément aux lois no 78-753 du 17 juillet 1978 précitée et no 79-18 du 3 janvier 1979 précitée.

Article 30

Sauf dispositions législatives contraires, les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la commission nationale, les personnes morales gérant un service public peuvent seules procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté.

Jusqu'à la mise en œuvre du fichier des conducteurs prévu par la loi no 70-539 du 24 juin 1970, les entreprises d'assurances sont autorisées, sous le contrôle de la commission, à traiter elles-mêmes les informations mentionnées à l'article 5 de ladite loi et concernant les personnes visées au dernier alinéa dudit article.

Article 31

Il est interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales (Loi no 92-1336 du 16 décembre 1992, art. 257) « ou les mœurs » des personnes.

Toutefois, les Églises ou les groupements à caractère religieux, philosophique, politique ou syndical peuvent tenir registre de leurs membres ou de leurs correspondants sous forme automatisée. Aucun contrôle ne peut être exercé, de ce chef, à leur encontre

Pour des motifs d'intérêt public, il peut aussi être fait exception à l'interdiction ci-dessus sur proposition ou avis conforme de la commission par décret en Conseil d'État.

Article 32

[Abrogé par la loi no 88-227 du 11 mars 1988, article 13] [3].

Article 33

Les dispositions des articles 24, 30 et 31 ne s'appliquent pas aux informations nominatives traitées par les organismes de la presse écrite ou audiovisuelle dans le cadre des lois qui les régissent et dans les cas où leur application aurait pour effet de limiter l'exercice de la liberté d'expression.

Article 33-1

(Inséré par la loi no 2000-321 du 12 avril 2000, article 5, 3°)

Les modalités d'application du présent chapitre sont fixées par décret en Conseil d'Etat pris après avis de la commission.

Chapitre V — Exercice du droit d'accès

Article 34

Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

Article 35

Le titulaire du droit d'accès peut obtenir communication des informations le concernant. La communication, en langage clair, doit être conforme au contenu des enregistrements.

Une copie est délivrée au titulaire du droit d'accès qui en fait la demande contre perception d'une redevance forfaitaire variable selon la catégorie de traitement dont le montant est fixé par décision de la commission et homologué par arrêté du ministre de l'Économie et des Finances.

Toutefois, la commission saisie contradictoirement par le responsable du fichier peut lui accorder :
— des délais de réponse ;
— l'autorisation de ne pas tenir compte de certaines demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique.

Lorsqu'il y a lieu de craindre la dissimulation ou la disparition des informations mentionnées au premier alinéa du présent article, et même avant l'exercice d'un recours juridictionnel, il peut être demandé au juge compétent que soient ordonnées toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Article 36

Le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le service ou organisme concerné doit délivrer sans frais copie de l'enregistrement modifié.

En cas de contestation, la charge de la preuve incombe au service auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord.

Lorsque le titulaire du droit d'accès obtient une modification de l'enregistrement, la redevance versée en application de l'article 35 est remboursée.

Article 37

Un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenue dans ce fichier.

Article 38

Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par la commission.

Article 39

En ce qui concerne les traitements intéressant la sûreté de l'État, la défense et la sécurité publique, la demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener toutes investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission.

Il est notifié au requérant qu'il a été procédé aux vérifications.

Article 40

Lorsque l'exercice du droit d'accès s'applique à des informations à caractère médical, celles-ci ne peuvent être communiquées à l'intéressé que par l'intermédiaire d'un médecin qu'il désigne à cet effet.

Chapitre V bis — Traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé

(Loi nº 94-548 du 1er juillet 1994, article 1er)

Article 40-1

Les traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de la présente loi, à l'exception des articles 15, 16, 17, 26 et 27.

Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients ne sont pas soumis aux dispositions du présent chapitre. Il en va de même des traitements permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif.

Article 40-2

Pour chaque demande de mise en œuvre d'un traitement de données, un comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, institué auprès du ministre chargé de la Recherche et composé de personnes compétentes en matière de recherche dans le domaine de la santé, d'épidémiologie, de génétique et de biostatistique, émet un avis sur la méthodologie de la recherche au regard des dispositions de la présente loi, la nécessité du recours à des données nominatives et la pertinence de celles-ci par rapport à l'objectif de la recherche, préalablement à la saisine de la Commission nationale de l'informatique et des libertés.

Le comité consultatif dispose d'un mois pour transmettre son avis au demandeur. À défaut, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours.

Le président du comité consultatif peut mettre en œuvre une procédure simplifiée.

La mise en œuvre du traitement de données est ensuite soumise à l'autorisation de la Commission nationale de l'informatique et des libertés, qui dispose, à compter de sa saisine par le demandeur, d'un délai de deux mois, renouvelable une seule fois, pour se prononcer. À défaut de décision dans ce délai le traitement de données est autorisé.

Article 40-3

Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données nominatives qu'ils détiennent dans le cadre d'un traitement automatisé de données autorisé en application de l'article 40-1.

Lorsque ces données permettent l'identification des personnes, elles doivent être codées avant leur transmission. Toutefois, il peut être dérogé à cette obligation lorsque le traitement de données est associé à des études de pharmacovigilance ou à des protocoles de recherche réalisés dans le cadre d'études coopératives nationales ou internationales ; il peut également y être dérogé si une particularité de la recherche l'exige. La demande d'autorisation comporte la justification scientifique et technique de la dérogation et l'indication de la période nécessaire à la recherche. A l'issue de cette période, les données sont conservées et traitées dans les conditions fixées à l'article 28. (Dernière phrase modifiée par la loi n° 2000-321 du 12 avril 2000, article 5, 4°).

La présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.

Les données sont reçues par le responsable de la recherche désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre le traitement. Ce responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci.

Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

Article 40-4

Toute personne a le droit de s'opposer à ce que des données nominatives la concernant fassent l'objet d'un traitement visé à l'article 40-1.

Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données.

Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

Article 40-5

Les personnes auprès desquelles sont recueillies des données nominatives ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :
1°) de la nature des informations transmises ;
2°) de la finalité du traitement de données ;
3°) des personnes physiques ou morales destinataires des données ;
4°) du droit accès et de rectification institué au chapitre V ;
5°) du droit d'opposition institué aux premier et troisième alinéas de l'article 40-4 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement.

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.

Dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées. Les dérogations à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point.

Article 40-6

Sont destinataires de l'information et exercent les droits prévus aux articles 40-4 et 40-5 les titulaires de l'autorité parentale, pour les mineurs, ou le tuteur, pour les personnes faisant l'objet d'une mesure de protection légale.

Article 40-7

Une information relative aux dispositions du présent chapitre doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données nominatives en vue d'un traitement visé à l'article 40-1.

Article 40-8

La mise en œuvre d'un traitement automatisé de données en violation des conditions prévues par le présent chapitre entraîne le retrait temporaire ou définitif, par la Commission nationale de l'informatique et des libertés, de l'autorisation délivrée en application des dispositions de l'article 40-2.

Il en est de même en cas de refus de se soumettre au contrôle prévu par le 2° de l'article 21.

Article 40-9

La transmission hors du territoire français de données nominatives non codées faisant l'objet d'un traitement automatisé ayant pour fin la recherche dans le domaine de la santé n'est autorisée, dans les conditions prévues à l'article 40-2, que si la législation de l'État destinataire apporte une protection équivalente à la loi française.

Article 40-10

Un décret en Conseil d'État précise les modalités d'application du présent chapitre.

Chapitre V ter — Traitement des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention

(Loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle, art. 41)

Art. 40-11

Les traitements de données personnelles de santé qui ont pour fin l'évaluation des pratiques de soins et de prévention sont autorisés dans les conditions prévues au présent chapitre.

Les dispositions du présent chapitre ne s'appliquent ni aux traitements de données personnelles effectuées à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie, ni aux traitements effectués au sein des établissements de santé par les médecins responsa-

bles de l'information médicale dans les conditions prévues au deuxième alinéa de l'article L. 710-6 du code de la santé publique.

Art. 40-12

Les données issues des systèmes d'information visés à l'article L. 710-6 du code de la santé publique, celles issues des dossiers médicaux détenus dans le cadre de l'exercice libéral des professions de santé, ainsi que celles issues des systèmes d'information des caisses d'assurance maladie, ne peuvent être communiquées à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention que sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées.

Il ne peut être dérogé aux dispositions de l'alinéa précédent que sur autorisation de la Commission nationale de l'informatique et des libertés dans les conditions prévues aux articles 40-13 à 40-15. Dans ce cas, les données utilisées ne comportent ni le nom, ni le prénom des personnes, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques.

Art. 40-13

Pour chaque demande, la commission vérifie 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. Elle s'assure 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 ou des activités de soins et de prévention. Elle vérifie que les données personnelles dont le traitement est envisagé ne comportent ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques. En outre, si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données personnelles dont le traitement est envisagé, la commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que des données ainsi réduites.

La commission détermine la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi.

Art. 40-14

La commission dispose, à compter de sa saisine par le demandeur, d'un délai de deux mois, renouvelable une seule fois, pour se prononcer. A défaut de décision dans ce délai, ce silence vaut décision de rejet. Les modalités d'instruction par la commission des demandes d'autorisation sont fixées par décret en Conseil d'Etat.

Les traitements répondant à une même finalité portant sur des catégories de données identiques et ayant des destinataires ou des catégories de destinataires identiques peuvent faire l'objet d'une décision unique de la commission.

Art. 40-15

Les traitements autorisés conformément aux articles 40-13 et 40-14 ne peuvent servir à des fins de recherche ou d'identification des personnes. Les personnes appelées à mettre en œuvre ces traitements, ainsi que celles qui ont accès aux données faisant l'objet de ces traitements ou aux résultats de ceux-ci lorsqu'ils demeurent indirectement nominatifs, sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

Les résultats de ces traitements ne peuvent faire l'objet d'une communication, d'une publication ou d'une diffusion que si l'identification des personnes sur l'état desquelles ces données ont été recueillies est impossible.

Chapitre VI — Dispositions pénales

Article 41 (Loi n° 92-1336 du 16 décembre 1992, art. 258)

Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Article 42 (Loi n° 92-1336 du 16 décembre 1992, art. 259)

Le fait d'utiliser le Répertoire national d'identification des personnes physiques sans l'autorisation prévue à l'article 18 est puni de cinq ans d'emprisonnement et de 2 000 000 F d'amende.

Article 43 (Loi n° 92-1336 du 16 décembre 1992, art. 260)

Est puni d'un an d'emprisonnement et de 100 000 F d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :
1°) Soit en s'opposant à l'exercice de vérifications sur place ;
2°) Soit en refusant de communiquer à ses membres, à ses agents ou aux magistrats mis à sa disposition, les renseignements et documents utiles à la mission qui leur est confiée par la commission ou en dissimulant lesdits documents ou renseignements, ou encore en les faisant disparaître ;
3°) Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements au moment où la demande a été formulée ou qui ne le présentent pas sous une forme directement intelligible.

Article 44 [Abrogé par la loi n° 92-1336 du 16 décembre 1992, art. 261]

Chapitre VII — Dispositions diverses

Article 45

Les dispositions des articles 25, 27, 28, 29, 29-1,30, 31, 32 et 33 relatifs à la collecte, à l'enregistrement et à la conservation des informations nominatives sont applicables aux fichiers non automatisés ou mécanographiques autres que ceux dont l'usage relève du strict exercice du droit à la vie privée.

Le premier alinéa de l'article 26 est applicable aux mêmes fichiers, à l'exception des fichiers publics désignés par un acte réglementaire.

Toute personne justifiant de son identité a le droit d'interroger les services ou organismes qui détiennent des fichiers mentionnés au premier alinéa du présent article en vue de savoir si ces fichiers contiennent des informations nominatives la concernant. Le titulaire du droit d'accès a le droit d'obtenir communication de ces informations ; il peut exiger qu'il soit fait application des trois premiers alinéas de l'article 36 de la présente loi relatifs au droit de rectification. Les dispositions des articles 37, 38, 39 et 40 sont également applicables. Un décret en Conseil d'État fixe les conditions d'exercice du droit d'accès et de rectification ; ce décret peut prévoir la perception de redevances pour la délivrance de copies des informations communiquées.

Le Gouvernement, sur proposition de la Commission nationale de l'informatique et des libertés, peut décider, par décret en Conseil d'État, que les autres dispositions de la présente loi peuvent, en totalité ou en partie, s'appliquer à un fichier ou à des catégories de fichiers non automatisés ou mécanographiques qui présentent,

soit par eux-mêmes, soit par la combinaison de leur emploi avec celui d'un fichier informatisé, des dangers quant à la protection des libertés.

Article 46

Des décrets en Conseil d'État fixeront les modalités d'application de la présente loi. Ils devront être pris dans un délai de six mois à compter de sa promulgation. Ces décrets détermineront les délais dans lesquels les dispositions de la présente loi entreront en vigueur. Ces délais ne pourront excéder deux ans à compter de la promulgation de ladite loi.

Article 47

La présente loi est applicable à Mayotte et aux territoires d'outre-mer (Loi n° 94-548 du 1er juillet 1994, art. 5) « à l'exception du chapitre V bis ».

Article 48

À titre transitoire, les traitements régis par l'article 15 ci-dessus, et déjà créés, ne sont soumis qu'à une déclaration auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues aux articles 16 et 17.

La commission peut toutefois, par décision spéciale, faire application des dispositions de l'article 15 et fixer le délai au terme duquel l'acte réglementant le traitement doit être pris.

À l'expiration d'un délai de deux ans à compter de la promulgation de la présente loi, tous les traitements régis par l'article 15 devront répondre aux prescriptions de cet article.

Liste des délibérations adoptées en 1999

Les délibérations sont publiées dans les chapitres du rapport, à la suite des commentaires qui les évoquent ou en annexe 6. 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	Objet
99-001 3 février 1999	Délibération portant désignation des membres de la Commission nationale de l'informatique et des libertés chargés d'exercer le droit d'accès indirect en application de l'article 39 de la loi du 6 janvier 1978
99-002 3 février 1999	Délibération portant élection du président, des vice-présidents et désignation du vice-président délégué de la Commission nationale de l'informatique et des libertés
99-003 3 février 1999	Délibération portant délégation d'attribution au président et au vice-président délégué de la Commission nationale de l'informatique et des libertés
99-004 18 février 1999 (cf. p. 241)	Délibération portant prorogation de l'expérimentation du formulaire de déclaration des traitements mis en œuvre dans le cadre d'un site web
99-005 18 février 1999 (cf. p. 241)	Délibération portant avis sur un projet de loi présenté par le ministre de l'Emploi et de la Solidarité relatif à la couverture maladie universelle et sur deux articles additionnels concernant l'un, le volet de santé de la carte électronique d'assurance maladie et l'autre, la réalisation de traitements de données personnelles de santé à des fins d'évaluation ou d'analyse du système de santé
99-006 9 mars 1999 (cf. p. 248)	Délibération portant avis favorable au projet de décret relatif à l'utilisation des informations figurant sur les relevés mensuels de contrats de travail temporaire par la direction de l'administration générale et de la modernisation des services du ministère de l'Emploi et de la Solidarité

Numéro date	Objet
99-007 9 mars 1999 (cf. p. 250)	Délibération portant avis favorable sur le projet de décision portant modification du traitement automatisé d'informations nominatives du 30 septembre 1992 de l'UNEDIC relatif au rapprochement des relevés mensuels des contrats de travail temporaire des déclarations des demandeurs d'emploi
99-008 9 mars 1999 (cf. p. 251)	Délibération portant avis favorable au projet d'acte réglementaire présenté par le ministère de l'Emploi et de la Solidarité relatif à une enquête sur le devenir des intérimaires et à l'établissement de la statistique annuelle du marché du travail
99-009 9 mars 1999 (cf. p. 253)	Délibération portant avis favorable au projet de décret présenté par le ministère de l'Emploi et de la Solidarité ayant pour finalité l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques contenu dans les relevés des missions de travail temporaire par la DARES pour la production de la statistique annuelle sur la population des intérimaires et pour l'enquête sur le devenir des intérimaires
99-010 9 mars 1999 (cf. p. 166)	Délibération décidant des vérifications sur place
99-011 9 mars 1999	Délibération décidant des vérifications sur place
99-012 9 mars 1999 (cf. p. 255)	Délibération portant avis sur le projet d'acte réglementaire présenté par le Conseil général de l'Ain et concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer l'aide sociale générale (ANIS-ASG)
99-013 9 mars 1999	Délibération décidant une vérification sur place
99-014 9 mars 1999	Délibération décidant une vérification sur place
99-015 9 mars 1999	Délibération décidant une mission de vérification sur place

Numéro date	Objet
99-016 9 mars 1999	Délibération décidant une mission de vérification sur place
99-017 25 mars 1999 (cf. p. 12)	Délibération relative aux suites à donner aux missions de contrôle auprès de l'association des guides et scouts d'Europe, de la société Serp, du journal « Français d'abord, le magazine de Jean-Marie Le Pen » et des légionnaires du Christ et portant dénonciation au Parquet
99-018 25 mars 1999 (cf. p. 257)	Délibération portant autorisation d'une enquête épidémiologique présentée par l'INSERM ayant pour finalité d'identifier et de suivre une cohorte d'enfants nés dans le canton de Beaumont-la-Hague entre 1953 et 1997 et ayant été scolarisés entre 1956 et 1997 afin de rechercher une éventuelle surincidence de leucémies et d'étudier la prévalence de malformations congénitales et portant avis sur un projet d'arrêté présenté par le secrétaire d'Etat à la Santé et à l'Action Sociale autorisant l'INSERM à utiliser le répertoire national inter-régimes des bénéficiaires de l'assurance-maladie
99-019 25 mars 1999 (cf. p. 260)	Délibération relative à la transmission d'informations fiscales par la direction générale des impôts à divers organismes de sécurité sociale et aux services des pensions de la direction générale de la comptabilité publique
99-020 25 mars 1999 (cf. p. 263)	Délibération concernant la transmission aux caisses de la mutualité sociale agricole d'informations relatives à la situation fiscale des bénéficiaires d'une pension de retraite ou d'invalidité
99-021 25 mars 1999 (cf. p. 265)	Délibération concernant la transmission aux centres régionaux des pensions de la direction générale de la comptabilité publique d'informations relatives à la situation fiscale des bénéficiaires d'une pension de retraite
99-022 25 mars 1999	Délibération portant sur une vérification sur place
99-023 8 avril 1999 (cf. p. 267)	Délibération portant avis sur le projet d'arrêté concernant la création par le ministère de l'Intérieur d'un traitement automatisé d'informations nominatives relatif à la délivrance des passeports

Numéro date	Objet
99-024 8 avril 1999 (cf. p. 24)	Délibération portant avis sur un projet d'arrêté du maire de Grenoble concernant l'envoi de courriers personnalisés aux administrés lors d'événements tels que les décès, naissances et mariages
99-025 22 avril 1999 (cf. p. 269)	Délibération portant modification : — de la norme simplifiée n° 36 concernant les traitements automatisés d'informations nominatives relatifs à la liquidation et au paiement des rémunérations des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public — de la norme simplifiée n° 37 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public
99-026 22 avril 1999 (cf. p. 270)	Délibération portant modification de la norme simplifiée n° 23 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des membres des associations à but non lucratif régies par la loi du 1er juillet 1901
99-027 22 avril 1999 (cf. p. 271)	Délibération concernant les traitements automatisés d'informations nominatives relatifs à la gestion des prêts de livres, de supports audiovisuels et d'œuvres artistiques et à la gestion des consultations de documents d'archives publiques
99-028 22 avril 1999 (cf. p. 274)	Délibération portant avis conforme sur un projet de décret présenté par le ministère de l'Emploi et de la Solidarité autorisant la caisse mutuelle d'assurance maladie des cultes (CAMAC) et la caisse mutuelle d'assurance vieillesse des cultes (CAMAVIC) à enregistrer des informations faisant apparaître directement ou indirectement l'appartenance religieuse de leurs assurés
99-029 4 mai 1999 (cf. p. 275)	Délibération portant avis sur un modèle-type de traitement présenté par le ministère de la Justice concernant le suivi des affaires pénales du parquet général des Cours d'Appel
99-030 4 mai 1999	Délibération décidant une mission de vérification sur place

Numéro date	Objet
99-031 4 mai 1999	Délibération décidant une mission de contrôle sur place
99-032 27 mai 1999 (cf. p. 277)	Délibération portant avis sur la mise en œuvre d'un traitement automatisé d'informations nominatives présenté par le comité opérationnel de lutte contre le travail illégal de Paris concernant la coordination de la lutte contre le travail illégal
99-033 24 juin 1999 (cf. p. 72)	Délibération portant avis sur un premier projet de décret en Conseil d'Etat pris pour l'application de l'article 107 de la loi du 30 décembre 1998
99-034 8 juillet 1999 (cf. p. 178)	Délibération relative aux suites à donner à la mission de contrôle sur place effectuée auprès des laboratoires Servier et portant dénonciation au Parquet
99-035 8 juillet 1999	Délibération décidant une mission de vérification sur place
99-036 8 juillet 1999 (cf. p. 279)	Délibération portant avis sur un projet de modification de 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 ou les forces d'occupation
99-037 8 juillet 1999 (cf. p. 281)	Délibération portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête « handicaps-incapacités-dépendances » menée auprès des ménages
99-038 8 juillet 1999 (cf. p. 282)	Délibération portant avis sur le projet d'acte réglementaire modificatif présenté par la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) concernant le traitement automatisé d'informations nominatives « ANAISS » (application nationale informatique des services sociaux)
99-039 8 juillet 1999	Délibération décidant une vérification sur place

Numéro date	Objet
99-040 8 juillet 1999	Délibération décidant une vérification sur place
99-041 8 juillet 1999 (cf. p. 285)	Délibération portant adoption du formulaire de déclaration des traitements de données personnelles mis en œuvre dans le cadre d'un site Internet
99-042 9 septembre 1999 (cf. p. 127)	Délibération relative à une demande d'avis présentée par l'institut de veille sanitaire concernant la mise en place à titre expérimental des déclarations obligatoires de séropositivité au virus de l'immunodéficience humaine
99-043 9 septembre 1999 (cf. p. 8)	Délibération portant modification de l'article 57 du règlement intérieur de la commission
99-044 23 septembre 1999	Délibération décidant une mission de vérification sur place
99-045 5 octobre 1999 (cf. p. 286)	Délibération portant avis sur un projet d'arrêté du ministre de l'Economie, des Finances et de l'Industrie concernant un traitement mis en œuvre par le service TRACFIN
99-046 14 octobre 1999	Délibération portant élection du vice-président et désignation du vice-président délégué de la Commission nationale de l'informatique et des libertés
99-047 14 octobre 1999 (cf. p. 80)	Délibération portant avis sur un projet de décret en Conseil d'Etat relatif aux mesures de sécurité prévues par l'article L.288 du livre des procédures fiscales
99-048 14 octobre 1999	Délibération portant adoption du rapport relatif au publipostage électronique et la protection des données personnelles
99-049 28 octobre 1999	Délibération décidant une mission de vérification sur place

Numéro date	Objet
99-050 28 octobre 1999 (cf. p. 289)	Délibération portant avis sur le projet d'arrêté, présenté par l'INSEE, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer les demandes de modification du NIR exprimées par les personnes nées en Algérie avant le 3 juillet 1962
99-051 28 octobre 1999 (cf. p. 290)	Délibération portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n° 82-103 du 2 janvier 1982 relatif au répertoire national d'identification des personnes physiques
99-052 28 octobre 1999 (cf. p. 36)	Délibération portant avis sur un projet de décret modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques
99-053 18 novembre 1999 (cf. p. 291)	Délibération portant avis sur le projet de règlement modifié du comité de réglementation bancaire relatif au fichier des incidents de remboursement des crédits aux particuliers (FICP)
99-054 18 novembre 1999 (cf. p. 293)	Délibération portant avis favorable au traitement automatisé d'informations nominatives mis en œuvre par le ministère de l'Agriculture et de la Pêche, à l'occasion du recensement général de l'agriculture (RGA)
99-055 18 novembre 1999 (cf. p. 295)	Délibération relative à la gestion et aux négociations des biens immobiliers
99-056 25 novembre 1999 (cf. p. 46)	Délibération portant avis sur les projets de décret en Conseil d'Etat relatifs aux mesures d'application de la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité et à l'informatisation des registres d'inscription des pactes civils de solidarité
99-057	*numéro non utilisé*
99-058 30 novembre 1999	Délibération décidant une vérification sur place

Numéro date	Objet
99-059 9 décembre 1999 (cf. p. 297)	Délibération portant adoption du rapport et des recommandations relatifs aux modalités d'informatisation de la surveillance épidémiologique du SIDA et en particulier de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine
99-060 9 décembre 1999 (cf. p. 91)	Délibération portant avis sur deux demandes d'avis modificatives prévoyant l'intégration du NIR dans les traitements « SPI » et « SIR »
99-061 21 décembre 1999 (cf. p. 148)	Délibération portant autorisation de mise en œuvre par la revue « Sciences et Avenir » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins
99-062 21 décembre 1999 (cf. p. 151)	Délibération portant autorisation de mise en œuvre par la revue « Le Figaro magazine » d'un traitement de données personnelles de santé à des fins d'analyse statistique des pratiques et des activités de soins

Délibérations adoptées en 1999, non publiées dans les chapitres du rapport

Délibération n° 99-004 du 18 février 1999 portant prorogation de l'expérimentation du formulaire de déclaration des traitements mis en œuvre dans le cadre d'un site Web

La Commission nationale de l'informatique et des libertés,

Vu la loi nº 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 nº 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 nº 87-25 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération nº 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 Web, annexé à la présente délibération ;

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 le 7 juillet 1998 (avis nº 98-075) un formulaire spécifiquement conçu pour la déclaration de tels traitements ;

Considérant que l'expérimentation de ce formulaire doit être prorogée jusqu'au 1er juillet 1999 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 ;

Décide de proroger jusqu'au 1er juillet 1999 l'expérimentation du modèle de formulaire de déclaration annexé à la présente délibération.

Délibération n° 99-005 du 18 février 1999 portant avis sur un projet de loi présenté par le ministre de l'Emploi et de la Solidarité relatif à la couverture maladie universelle et sur deux articles additionnels concernant l'un, le volet de santé de la carte électronique d'assurance maladie et l'autre, la réalisation de traitements de données personnelles de santé à des fins d'évaluation ou d'analyse du système de santé

La Commission Nationale de l'Informatique et des Libertés,

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 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 relative à l'Informatique, aux fichiers et aux libertés modifiée ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée et notamment son article 20 ;

Vu l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ;

Vu le code de la sécurité sociale ;

Vu le code de la santé publique ;

Vu le projet de loi présenté par le Ministre de l'Emploi et de la Solidarité relatif à la couverture maladie universelle ;

Après avoir entendu Monsieur Maurice VIENNOIS 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, conformément aux dispositions de l'article 20 du décret n° 78-774 du 17 juillet 1978, d'un projet de loi relatif à la couverture maladie universelle et de deux articles additionnels portant d'une part sur le volet santé de la carte électronique d'assurance maladie et d'autre part sur la réalisation de traitements de données personnelles de santé à des fins d'évaluation ou d'analyse du système de santé ;

Sur le projet de loi relatif à la couverture maladie universelle

Considérant que le dispositif proposé vise à garantir à toute personne, quelle que soit sa situation, une protection contre le risque maladie, par le rattachement à un régime obligatoire d'assurance maladie ; qu'ainsi toute personne disposant en France d'une résidence stable et régulière, et ne bénéficiant pas déjà de droits à un régime obligatoire, sera obligatoirement affiliée au régime général, à charge ensuite pour la caisse primaire d'assurance maladie de rechercher le régime dont est susceptible de relever l'intéressé (article 3.1 : futur article L380.I) ;

Considérant que pour bénéficier de l'affiliation automatique au régime général, les personnes concernées devront présenter leur demande auprès d'une caisse primaire d'assurance maladie (article 4, futur article L161-2-1) ; que les caisses seront donc amenées à recueillir auprès des intéressés des renseignements portant notamment sur leur situation professionnelle et à leur demander des justificatifs de domicile ; que cette collecte nouvelle d'informations dès lors qu'elle se traduira par un enrichissement du contenu des fichiers informatiques des caisses, devra être soumise à la CNIL ;

Considérant que l'entrée en application du dispositif de la couverture maladie universelle devrait se traduire par une augmentation du volume des fichiers des organismes d'assurance maladie et par de nouveaux échanges d'informations ;

Considérant que le projet de loi prévoit également au bénéfice des personnes dont les revenus ne dépassent pas un certain montant, la prise en charge du ticket modérateur et du forfait journalier ainsi que des modalités de remboursement adaptées pour les prothèses, notamment en matière dentaire et

optique ; que les bénéficiaires de cette protection complémentaire pourront également bénéficier de la dispense d'avance de frais totale ;

Considérant que cette couverture complémentaire sera servie soit, pour le compte de l'Etat, par les organismes d'assurance maladie, soit par l'organisme de couverture complémentaire choisi par le bénéficiaire ; que pour obtenir le droit à cette protection les personnes intéressées devront présenter leur demande auprès de la caisse d'assurance maladie dont elles dépendent, accompagnée des renseignements et justificatifs nécessaires s'agissant en particulier du montant des ressources, de la situation familiale, de la résidence du demandeur et des membres de sa famille (article 22.1 : futur article L 861.III) ;

Considérant que les caisses seront donc amenées à recueillir et à enregistrer dans leurs fichiers des informations supplémentaires sur les ressources dont disposent les demandeurs et les membres de leur famille ;

Considérant en outre que le projet de loi prévoit que pour la détermination du droit à cette couverture et le contrôle des déclarations de ressources effectuées à cette fin, les organismes d'assurance maladie pourront demander toutes les informations nécessaires aux organismes d'indemnisation du chômage (ASSEDIC) qui seront tenus de les leur communiquer ;

Considérant que l'article 22-III introduisant un nouvel article L861-10 au code de la sécurité sociale précise que les informations demandées devront être limitées aux données strictement nécessaires à l'accomplissement de cette mission ;

Considérant que les personnes concernées devront, conformément aux dispositions de la loi du 6 janvier 1978, être clairement informées de la mise en place de ces échanges d'informations ; que s'il appartiendra à la Commission de s'assurer de l'effectivité de ces mesures d'information lors de l'accomplissement des formalités préalables à la mise en place de ces échanges, il conviendrait toutefois que la loi en prévoit le principe ou renvoie à un décret d'application le soin d'en fixer les modalités ;

Considérant que dans la mesure où le projet de loi prévoit que les personnes titulaires de l'aide médicale bénéficieront de plein droit de la couverture complémentaire, l'application de cette mesure devrait se traduire par des transferts d'informations entre d'une part, les Conseils Généraux et les DDASS qui disposent des fichiers des bénéficiaires de l'aide médicale et d'autre part, les caisses d'assurance maladie qui mettront en œuvre à cet effet des traitements automatisés d'informations nominatives (articles 29 et 30 du projet de loi) ;

Considérant en conséquence que l'article 30 pourrait être complété de la façon suivante : « pour la mise en œuvre de l'article 29, les organismes d'assurance maladie reçoivent de l'Etat ou des départements concernés les informations nominatives nécessaires et mettent en œuvre, dans les conditions prévues par la loi du 6 janvier 1978, des traitements automatisés d'informations nominatives » ;

Considérant que le texte soumis à la Commission prévoit le maintien de l'aide médicale pour les personnes résidant en France mais ne remplissant pas les conditions nécessaires pour bénéficier de la couverture maladie universelle et institue, en ce domaine, un transfert de compétences des Conseils Généraux vers l'Etat, celui-ci prenant désormais en charge l'ensemble des dépenses d'aide médicale ; qu'il incombera exclusivement au représentant

de l'Etat dans le département ou par délégation au directeur de la caisse primaire d'assurance maladie de prononcer l'admission à l'aide médicale ;

Considérant que l'application de ces dispositions devrait se traduire par des transferts d'informations nominatives entre les conseils généraux, les DDASS et les caisses d'assurance maladie et qu'il conviendra que la Commission en soit saisie ;

Considérant que dans la mesure où la mise en place de ce dispositif pourrait conduire à des échanges d'informations comportant notamment le NIR des personnes concernées, il y a lieu de rappeler que ces traitements devront être strictement soumis aux limites et conditions définies par la législation et la réglementation en vigueur ;

Emet un avis favorable aux dispositions du projet de loi consacrées à la couverture maladie universelle en proposant que :
— la loi précise que les personnes seront informées des échanges d'informations prévus à l'article 22.III (futur article L 861.10) ou renvoie à un décret d'application le soin de fixer les modalités de cette information ;
— l'article 30 soit complété de la façon suivante : « pour la mise en œuvre de l'article 29, les organismes d'assurance maladie reçoivent de l'Etat ou des départements concernés les informations nominatives nécessaires et mettent en œuvre, dans les conditions prévues par la loi du 6 janvier 1978, des traitements automatisés d'informations nominatives » ;

Sur le volet de santé de la carte d'assurance maladie

Considérant que le ministère de l'emploi et de la solidarité saisit la CNIL d'un article additionnel au projet de loi sur la couverture maladie universelle portant sur le volet de santé de la carte électronique d'assurance maladie ;

Considérant en effet que le Conseil d'Etat dans un arrêt du 3 juillet 1998, par lequel il a annulé l'arrêté du 28 mars 1997 portant approbation de la convention nationale des médecins généralistes, a estimé qu'il revenait au législateur de déterminer les modalités de mise en œuvre du volet médical et de fixer dans la loi « les garanties nécessaires à la protection des droits individuels, qu'il s'agisse notamment du consentement du patient à l'enregistrement des données le concernant, du délai pendant lequel les informations doivent demeurer sur le » volet santé « et de la possibilité d'en obtenir la suppression » ;

Considérant que le volet de santé de la carte ainsi porté sur un support électronique est institué dans l'intérêt du titulaire de la carte ; que ses finalités sont définies au paragraphe II du futur article L 161-31 du code de la sécurité sociale qui lui-même renvoie au futur article L162-1-6 la définition du contenu et des modalités d'utilisation du volet de santé ;

Considérant que le paragraphe I du futur article L 162-1-6 du code de la sécurité sociale dispose que « sous réserve du droit d'opposition du titulaire de la carte ou de son représentant légal et sauf impossibilité matérielle, chaque professionnel de santé habilité, conformément au 2° du IV du présent article, et dispensant des soins au titulaire de la carte doit obligatoirement porter sur le volet de santé les informations nécessaires à la prise en charge de l'urgence, à la continuité et à la coordination des soins, dans l'intérêt du titulaire » ; que les données appelées à figurer sur le volet de santé seront fixées par décret en Conseil d'Etat pris après avis du Conseil National de l'Ordre des médecins et de la CNIL ;

Considérant que pour assurer les garanties nécessaires à la protection des droits individuels, il importe que l'enregistrement des informations dans le volet de santé de la carte s'effectue après accord du titulaire de la carte ; qu'en outre la rédaction retenue, en ce qu'elle paraît par l'emploi du terme « obligatoirement », mettre à la charge du professionnel de santé concerné une obligation d'inscription sur le volet médical sans égard pour les droits des patients pourrait laisser planer un doute sur l'effectivité de ces droits ;

Considérant en conséquence que le paragraphe I du futur article L 162-1-6 du code de la sécurité sociale devrait être rédigé de la façon suivante :

« Après accord du patient ou de son représentant légal, chaque professionnel de santé habilité conformément au 2° du IV du présent article, porte sur le volet de santé les informations qu'il estime nécessaires à la prise en charge de l'urgence, à la continuité et à la coordination des soins, dans l'intérêt du titulaire ».

Considérant que le projet de texte soumis à la Commission dispose également que « le titulaire de la carte peut avoir accès, par l'intermédiaire d'un professionnel de santé lui dispensant des soins et pour les informations auxquelles ce professionnel a lui-même accès, au contenu du volet de santé de sa carte » ;

Considérant que cette rédaction est plus restrictive que celle de l'article 40 de la loi du 6 janvier 1978 qui prévoit que le droit d'accès aux informations à caractère médical s'exerce par l'intermédiaire d'un médecin choisi par l'intéressé ;

Considérant que le souci de rendre plus aisé le droit d'accès du patient aux données médicales inscrites sur sa carte devrait conduire à rédiger en ces termes le projet de disposition : « le titulaire de la carte peut avoir accès, par l'intermédiaire d'un professionnel de santé de son choix, habilité conformément au 2° du IV du présent article et pour les informations auxquelles ce professionnel a lui-même accès, au contenu du volet de santé de sa carte » ;

Considérant ainsi que le titulaire de la carte pourra consulter le contenu intégral du volet médical de sa carte auprès de ces professionnels de santé ; que cette garantie essentielle doit être mise en œuvre dans des conditions assurant la confidentialité de ces informations vis à vis des tiers ; qu'il convient à ce titre que la loi précise qu'aucune copie de ces informations ne pourra être délivrée au patient, afin que nul ne puisse exiger de celui-ci, dans des circonstances étrangères à la relation de soins, la production d'un « certificat de bonne santé » ;

Considérant que le texte soumis à la Commission dispose que « le titulaire de la carte peut conditionner l'accès à une partie du volet de santé de sa carte à la frappe d'un code secret qu'il aura lui-même défini » ; qu'il appartiendra au titulaire de la carte de déterminer celles des informations qu'il souhaite voir protégées par ce code personnel ; que seuls les professionnels de santé habilités conformément au paragraphe IV-2° de l'article L 162-1-6 du code de la sécurité sociale pourront consulter, inscrire ou effacer les informations figurant sur le volet santé ; à l'occasion de la dispensation des soins ou de la délivrance de prestations ; qu'un décret en Conseil d'Etat pris après avis du Conseil National de l'Ordre des médecins et de la Commission Nationale de l'Informatique et des Libertés déterminera les conditions d'application de ces dispositions ;

Considérant, s'agissant de la durée de conservation des informations portées sur le volet de santé, qu'il résulte du texte soumis à la Commission, que le titulaire de la carte pourra obtenir, à tout moment, en s'adressant à un médecin habilité, la suppression des informations précédemment portées sur le volet médical ;

Emet un avis favorable à l'article 36 du projet de loi relatif au volet de santé de la carte d'assurance maladie, en proposant que :
— le paragraphe I du futur article L 162-1-6 du code de la sécurité sociale soit rédigé de la façon suivante : « Après accord du patient ou de son représentant légal, chaque professionnel de santé habilité conformément au 2° du IV du présent article porte sur le volet de santé les informations qu'il estime nécessaires à la prise en charge de l'urgence, à la continuité et à la coordination des soins, dans l'intérêt du titulaire » ;
— le 2e alinéa du paragraphe II de l'article 36 soit rédigé en ces termes : « le titulaire de la carte peut avoir accès, par l'intermédiaire d'un professionnel de santé de son choix, habilité conformément au 2° du IV du présent article et pour les informations auxquelles ce professionnel a lui-même accès, au contenu du volet de santé de sa carte. Aucune copie ne peut être délivrée. »

Sur la réalisation de traitements de données personnelles de santé à des fins d'évaluation ou d'analyse du système de santé :

Considérant que le texte soumis à l'avis de la CNIL a pour objet de préciser les conditions dans lesquelles des données de santé indirectement nominatives, qu'elles soient fournies par les professionnels de santé, les systèmes d'information hospitaliers ou les traitements des caisses de sécurité sociale, peuvent être diffusées et exploitées à des fins d'analyse des activités de soins et de prévention ou d'évaluation des pratiques de soins et de prévention ;

Considérant qu'à cet effet, il serait institué, pour cette catégorie de traitement une procédure spécifique d'autorisation voisine de celle prévue au chapitre V bis de la loi du 6 janvier 1978 relatif aux traitements de recherche dans le domaine de la santé ;

Considérant en effet, que préalablement à la saisine de la CNIL, tout organisme, à l'exception des organismes d'assurance maladie et des établissements de santé, souhaitant créer un traitement automatisé ayant pour fins l'évaluation des activités ou pratiques de soins devrait recueillir l'avis d'un comité placé auprès des ministres chargé de la santé et de la sécurité sociale et qui serait composé de représentants des ministères précités, des organismes d'assurance maladie, des ordres professionnels, de personnes qualifiées et d'usagers de la santé ; que ce comité serait chargé d'apprécier « les garanties de sérieux et les références du demandeur ainsi que la conformité de sa demande à des missions ou à son objet social, la pertinence du traitement au regard de la finalité d'évaluation, la nécessité de recourir à des données personnelles et la durée de conservation des données » ; qu'en outre, les traitements qu'ils émanent d'un organisme public ou d'un organisme privé, ne pourraient être mis en œuvre qu'après autorisation de la CNIL, le silence de la Commission, après un délai de deux mois valant refus ;

Considérant que le texte présenté prévoit également un certain nombre de garanties destinées à éviter tout risque d'identification indirecte des personnes ;

Considérant que l'alourdissement qui résulterait de la mise œuvre de cette nouvelle procédure parait excessif au regard des traitements concernés qui

n'utilisent, à la différence des données traitées à des fins de recherche, que des données indirectement nominatives, l'identité des personnes n'étant jamais communiquée aux organismes susceptibles de mettre en œuvre les traitements concernés ;

Considérant en outre que le texte proposé, par son imprécision, est de nature à provoquer des conflits de compétences entre le nouveau comité et le comité consultatif pour le traitement de l'information en matière de recherche dans le domaine de la santé, institué par la loi du 1er juillet 1994 ; que de surcroît, dans certains cas, un cumul de formalités pourrait être redouté ; que d'ailleurs la composition du comité proposé qui associerait aux experts scientifiques, des usagers de la santé, voire des ordres professionnels laisse planer un doute sur les missions exactes qui seraient les siennes ;

Considérant enfin que les délais prévisibles de mise en œuvre d'une nouvelle procédure « sui generis » de déclaration de traitement à la CNIL et la perspective de la prochaine transposition de la directive européenne du 24 octobre 1995 peuvent légitimement faire douter de l'impact réel d'une réforme présentée comme urgente et nécessaire ;

Considérant que les objectifs du texte proposé paraissent pouvoir être atteints par d'autres voies dès lors que la loi poserait le principe que les traitements de données réalisés à des fins d'analyse des activités de soins et de prévention ou d'évaluation des pratiques de soins et de prévention ne comporteraient en aucun cas ni le nom ni le prénom ni le numéro d'inscription au répertoire national d'identification des personnes physiques ; qu'en outre les modalités de leur diffusion ne devraient pas permettre l'identification des personnes sous peine de sanctions pénales ; qu'enfin, le traitement de ces données très indirectement nominatives continuerait à relever des procédures prévues par la loi du 6 janvier 1978 dans leur forme actuelle ;

Emet un avis défavorable à l'article 40 du projet de loi et estime que cet article devrait être rédigé de la façon suivante :

« Les données issues des systèmes d'information visés à l'article L 710-6 du code de la santé publique, ainsi que celles issues des systèmes d'information des caisses d'assurance maladie sont transmises, sous une forme garantissant l'anonymat des personnes concernées, aux services des ministères chargés des affaires sociales et de la santé, aux agences régionales de l'hospitalisation, aux organismes d'assurance maladie, ainsi qu'aux organismes chargés d'une mission d'évaluation des pratiques de soins et de prévention ou d'analyse des activités de soins et de prévention dont la liste est fixée par décret en Conseil d'Etat.

Toutefois, les organismes précités peuvent être, pour l'exercice de leur mission, destinataires de données personnelles sous réserve que ces données ne comportent ni le nom, ni le prénom du patient, ni le numéro d'inscription au répertoire national d'identification des personnes physiques. Le traitement de ces données par l'administration ou l'organisme destinataire s'effectue dans le respect des dispositions de la loi du 6 janvier 1978 modifiée.

Ces données peuvent également être communiquées, dans les mêmes conditions à des personnes ou organismes autres que ceux visés au deuxième alinéa, sur décision des ministres des affaires sociales et de la santé prise après avis d'un comité technique d'experts. La composition de ce comité est fixée par décret en Conseil d'Etat.

Les traitements par les organismes visés à l'alinéa précédent de données ainsi communiquées s'effectuent, quelque soit la qualité des organismes, dans le respect des dispositions de la loi du 6 janvier 1978 modifiée et ne peuvent en aucune façon servir à des fins de recherche ou d'identification des personnes.

Les résultats de ces traitements ne peuvent faire l'objet d'une communication, d'une publication ou d'une diffusion que si l'identification des personnes sur l'état de santé desquelles ces données ont été recueillies est impossible. Tout manquement à ces dispositions est réprimé par les peines prévues à l'article 226-22 du code pénal.

Les services de l'Etat et les services des organismes gérant un régime de base d'assurance maladie mettent à la disposition du public dans des conditions garantissant l'anonymat des personnes concernées les données statistiques nécessaires à son information, issues des traitements qu'ils effectuent à des fins d'évaluation des pratiques de soins et de prévention ou d'analyse des activités de soins et de prévention. A cet effet, un programme annuel de production de ces statistiques est fixé par arrêté des ministres de la santé et de la sécurité sociale ».

Délibération n° 99-006 du 9 mars 1999 portant avis favorable au projet de décret relatif à l'utilisation des informations figurant sur les relevés mensuels de contrats de travail temporaire par la direction de l'administration générale et de la modernisation des services du ministère de l'Emploi et de la Solidarité

(Demande d'avis n° 631397)

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 les articles L 124-11 et R 124-4-1 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 projet de décret relatif à l'utilisation des informations figurant sur les relevés mensuels de contrats de travail temporaire par la direction de l'administration générale et de la modernisation des services du ministère de l'emploi et de la solidarité ;

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 Commission est saisie par la direction de l'administration générale et de la modernisation des services du ministère de l'emploi et de la solidarité d'un projet de décret relatif à l'utilisation des informations figurant sur les relevés mensuels de contrats de travail temporaire ;

Considérant que conformément aux dispositions de l'article L 124-11 du code du travail, les services déconcentrés du ministère de l'emploi et de la solidarité sont destinataires des informations contenues dans les relevés mensuels de missions de travail temporaire par l'intermédiaire de la direction de l'administration générale et de la modernisation des services (DAGEMO) du ministère de l'emploi et de la solidarité ;

Considérant que la DAGEMO reçoit de l'UNEDIC la totalité des relevés des missions de travail temporaire et se charge de les adresser à chaque DDTEFP pour les missions de contrôle qui leur incombent ;

Considérant que dans chaque DDTEFP, le service du contrôle de la recherche d'emploi est chargé de s'assurer de la réalité de la recherche d'emploi des demandeurs d'emploi et de contrôler les situations de cumul entre recherche d'emploi et travail temporaire, en particulier de s'assurer que les déclarations produites mensuellement par les demandeurs d'emploi comportent bien l'indication des missions de travail temporaire éventuellement effectuées ;

Considérant que dans chaque DDTEFP les sections d'inspection du travail contrôlent le respect des dispositions sur le travail temporaire notamment la durée des missions ainsi que les motifs du recours au travail temporaire ;

Considérant que la DAGEMO transmet actuellement ces informations aux DDTEFP sous forme de listing papier ; que cette forme de transmission est onéreuse et en grande partie inexploitable ; qu'elle souhaite les transmettre sur cédérom afin de rendre effective l'utilisation des informations transmises aux directions départementales ;

Considérant que seuls les destinataires habilités des sections d'inspection du travail et au service du contrôle de la recherche d'emploi disposant d'un nom d'utilisateur et d'un mot de passe auraient accès aux informations les concernant et qu'il serait en particulier impossible d'accéder aux informations relatives aux autres départements ;

Considérant que la nature des informations adressées aux directions départementales de l'emploi ne sera pas modifiée par le changement de support ;

Considérant que les informations transmises sont pour les établissements de travail temporaire, le numéro SIRET, la raison sociale, l'adresse complète, le numéro de téléphone, la date du premier emploi intérimaire, le nombre de contrats conclus, le nombre de contrats en cours et le nombre d'établissements utilisateurs ; pour l'établissement utilisateur le numéro SIRET, la raison sociale, l'adresse complète, le code APE, la raison sociale du lieu d'exécution des missions, l'adresse complète du lieu d'exécution des missions ; pour le salarié : le nom, le prénom, le code postal du domicile, la nationalité et le NIR, le code emploi et la qualification, les dates de début et de fin de contrat ;

Considérant que ces informations seront conservées pendant une durée de trois ans ;

Considérant que les contrôles à effectuer par les sections d'inspection du travail rendent cette durée de trois ans adéquate et non excessive ;

Considérant que les intérimaires sont d'ores et déjà informés de ces transmissions d'informations par un affichage dans chaque établissement de travail temporaire

prévu par l'article R 124-4-1 du code du travail ; qu'ainsi les intérimaires sont informés de la communication d'informations nominatives contenues dans les relevés mensuels de situation à l'UNEDIC et aux DDTEFP, ainsi que l'existence d'un droit d'accès et de rectification auprès de ces organismes ;

Emet un avis favorable au projet de décret présenté par la direction de l'administration générale et de la modernisation des services du ministère de l'emploi et de la solidarité.

Délibération n° 99-007 du 9 mars 1999 portant avis favorable sur le projet de décision portant modification du traitement automatisé d'informations nominatives du 30 septembre 1992 de l'UNEDIC relatif au rapprochement des relevés mensuels des contrats de travail temporaire des déclarations des demandeurs d'emploi

(Demande d'avis n° 618190)

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 les articles L 124-11 et R 124-4 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 92-968 du 7 septembre 1992 modifiant le 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 ;

Vu la délibération n° 92-070 du 7 juillet 1992 relative à un projet d'acte réglementaire présenté par l'UNEDIC relatif à un traitement automatisé d'informations nominatives ayant pour finalité le rapprochement des relevés mensuels des contrats des entreprises de travail temporaire de déclarations faites par les demandeurs d'emploi, ainsi que l'établissement de statistiques ;

Vu le projet de décision présenté par l'UNEDIC portant modification du traitement d'informations nominatives du 30 septembre 1992 relatif au rapprochement des relevés mensuels des contrats de travail temporaire des demandeurs d'emploi ;

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 traitement de l'UNEDIC ayant pour finalité le rapprochement des relevés mensuels des contrats des entreprises de travail temporaire des déclarations faites par les demandeurs d'emploi ayant fait l'objet d'un

avis favorable de la Commission le 7 juillet 1992 a connu depuis lors plusieurs modifications ;

Considérant que les modifications apportées au traitement portent sur la nature des informations faisant l'objet de transmission à la DARES ainsi que sur l'ajout de nouveaux destinataires ;

Considérant que l'UNEDIC reçoit des entreprises de travail temporaire tous les 20 du mois conformément à la délibération de la CNIL du 7 juillet 1992, le numéro SIRET, la raison sociale, l'adresse complète de l'entreprise de travail temporaire et son numéro de téléphone, le numéro SIRET et le code APE, la raison sociale, l'adresse complète de l'établissement utilisateur, le nom, le prénom, le code postal du domicile, la nationalité et le NIR du titulaire du contrat ainsi que les dates de début et de fin du contrat de travail, le salaire brut et la qualification professionnelle ;

Considérant que la DARES est, aux termes de la délibération précitée, destinataire du code nationalité du salarié, du sexe, du mois et de l'année de naissance, du code postal du domicile, du code emploi, de la qualification professionnelle, des dates de début et de fin du contrat de travail, du code APE et du numéro de département de l'entreprise utilisatrice ;

Considérant que la DARES souhaite, en plus de ces information et afin d'établir la statistique annuelle du marché du travail, être destinataire du numéro SIRET de l'entreprise de travail temporaire et du numéro de département, du numéro SIRET de l'établissement utilisateur, de son code APE et du numéro du département, du département du domicile du salarié, de sa nationalité, du code emploi et du NIR du salarié ;

Considérant que le projet de décret relatif à l'utilisation par la DARES du répertoire national d'identification des personnes physiques contenu dans les relevés mensuels de contrats de travail temporaire pour l'établissement de sa statistique annuelle du marché du travail a recueilli un avis favorable par la délibération 99 -009 du 09 mars 1999 ;

Emet un **avis favorable** au projet de décision présenté par l'UNEDIC.

Délibération n° 99-008 du 9 mars 1999 portant avis favorable au projet d'acte réglementaire présenté par le ministère de l'Emploi et de la Solidarité relatif à une enquête sur le devenir des intérimaires et à l'établissement de la statistique annuelle du marché du travail

(Demande d'avis n° 607571)

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 et notamment son article 18 ;

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

Vu le décret nº 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le projet de décision présenté par la Direction de l'animation, de la recherche et des études statistiques portant sur l'enquête sur le devenir des intérimaires ;

Vu la délibération 99-007 du 09 mars 1999 portant avis favorable sur le projet de décision de l'UNEDIC portant modification du traitement automatisé d'informations nominatives relatif au rapprochement des relevés mensuels des contrats de travail temporaire des déclarations des demandeurs d'emploi ;

Vu la délibération 99-0009 du 09 mars 1999 portant avis favorable au projet de décret relatif à l'utilisation du répertoire national d'identification des personnes physiques contenus dans les relevés des missions de travail temporaire par la DARES pour l'établissement de la statistique annuelle du marché du travail et dans le cadre de l'enquête sur le devenir des intérimaires ;

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 Direction de l'Animation de la Recherche et des Études Statistique du ministère de l'emploi et de la solidarité (DARES) a déposé une demande d'avis concernant une enquête relative au devenir des intérimaires ;

Considérant que l'enquête prendra la forme d'entretiens réalisés en face à face sur un échantillon de 260 personnes, composé de deux cohortes ; que la première cohorte est composée de personnes ayant effectué des missions en juillet et août 1998 ;

Considérant que l'échantillon est constitué à partir des informations relatives aux missions de travail temporaire réalisées sur la période en cause que l'UNEDIC transmet à la DARES tous les mois ;

Considérant que l'UNEDIC reçoit des entreprises de travail temporaire tous les mois le récapitulatif des missions effectuées ou achevées au cours du mois précédent ; que cette transmission a fait l'objet d'un avis favorable de la Commission par la délibération 92-070 du 7 juillet 1992 modifiée par la délibération 99-007 du 09 mars 1999 ;

Considérant que la DARES est destinataire d'informations statistiques lui permettant d'établir la statistique annuelle du marché du travail : code nationalité du salarié, sexe, mois et année de naissance, code postal du domicile, code emploi, qualification professionnelle, dates de début et fin de contrat de travail, code APE et numéro de département de l'entreprise utilisatrice ;

Considérant que la DARES souhaite obtenir en plus de ces informations statistiques d'une part, le nom, l'adresse de l'intérimaire et le nom des agences de travail temporaires ; que ces informations nominatives paraissent pertinentes, afin de réaliser cette enquête ponctuelle ;

Considérant que dans la mesure où il s'agit d'une enquête facultative, les personnes concernées seront informées au préalable de la transmission de leurs coordonnées au sous-traitant de la DARES et auront la possibilité de s'opposer à faire partie de l'échantillon ; que toutes les mesures de sécurité prises sont satisfaisantes et que la durée de conservation des données sous forme nominative n'excédera pas le temps de dépouillement de la deuxième série d'entretiens ;

Considérant que la DARES souhaite également disposer du NIR des intérimaires pour cette enquête ponctuelle afin de constituer les cohortes des personnes interrogées en fonction de leur appartenance aux différentes catégories d'intérimaires (missions d'été, missions régulières en dehors des périodes d'été) ;

Considérant que le NIR permettrait également d'apparier la liste des personnes retenues pour composer l'échantillon avec un extrait du fichier UNEDIC comportant les nom, prénom et code postal des intérimaires afin, par dédoublonnage, de s'assurer de la qualité de l'échantillon qui ne doit pas comporter deux fois la même personne ;

Considérant que l'utilisation du NIR des intérimaires est limitée pour cette enquête à la constitution de l'échantillon et au rapprochement des fichiers de l'UNEDIC afin de recueillir les noms et adresses des personnes faisant l'objet de l'enquête ;

Considérant que la DARES fera appel à un sous-traitant qui ne devra pas recevoir d'autres informations que celles prévues dans le cahier des clauses techniques particulières annexé au contrat de passation de marché ; qu'il s'agit du nom et de l'adresse de l'établissement utilisateur, du nom, du prénom et du code postal du domicile des personnes ayant accepté l'entretien ;

Considérant par ailleurs, que la DARES souhaite être destinataire des informations suivantes afin d'établir la statistique annuelle du marché du travail : numéro SIRET et du département de l'établissement de travail temporaire, le numéro SIRET de l'établissement utilisateur et le NIR du salarié ;

Considérant que l'utilisation de ce numéro sera limitée à l'attribution des différentes missions effectuées à l'intérimaire en cause ;

Considérant que, hormis dans le cas de l'enquête sur le devenir des intérimaires où le fichier de l'échantillon sera croisé avec le fichier de l'UNEDIC afin de recueillir les nom et adresses des personnes susceptibles d'être enquêtées, il ne sera fait aucun rapprochement avec aucun autre fichier de quelque provenance que ce soit ;

Emet un **avis favorable** au projet de décision présenté par la DARES relative à l'enquête sur le devenir des intérimaires.

Délibération n° 99-009 du 9 mars 1999 portant avis favorable au projet de décret présenté par le ministère de l'Emploi et de la Solidarité ayant pour finalité l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques contenu dans les relevés des missions de travail temporaire par la DARES pour la production de la statistique annuelle sur la population des intérimaires et pour l'enquête sur le devenir des intérimaires

(Demande d'avis nº 607571)

La Commission nationale de l'informatique et des libertés ;

Vu la Convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et notamment son article 18 ;

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

Vu le projet de décret présenté par le ministère de l'emploi et de la solidarité ayant pour finalité l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques contenu dans les relevés de missions de travail temporaire par la Direction de l'Animation, de la Recherche et des Etudes Statistiques dans l'établissement de sa statistique annuelle du marché du travail et pour l'enquête sur le devenir des intérimaires ;

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 Direction de l'Animation, de la Recherche et des Etudes Statistiques souhaite être destinataire du numéro d'inscription au répertoire national d'identification des personnes physiques des intérimaires qui figure dans les relevés de mission de travail temporaire que lui transmet l'UNEDIC pour l'élaboration de l'ensemble de ses statistiques annuelles sur la population des intérimaires ainsi que ponctuellement pour réaliser une enquête particulière relative au devenir des intérimaires ;

Considérant que s'agissant de l'enquête qualitative, l'utilisation du NIR permettrait de constituer les cohortes des personnes interrogées en fonction de leur appartenance aux différentes catégories d'intérimaires : ceux ayant de nombreuses missions, ceux concentrant leurs missions l'été et ceux n'exerçant qu'un type de mission ou n'étant employés que par un seul établissement de façon récurrente ; que le NIR permettrait également d'apparier la liste des personnes retenues pour composer l'échantillon avec un extrait du fichier UNEDIC comportant les nom, prénom et code postal des intérimaires afin, par dédoublonnage, de s'assurer de la qualité de l'échantillon qui ne doit pas comporter deux fois la même personne ;

Considérant que s'agissant de la statistique annuelle du marché du travail, la DARES fait valoir que l'utilisation du NIR permettrait de rendre compte de l'hétérogénéité de la population des intérimaires, d'établir la pyramide des âges et de faire apparaître les qualifications assurant une bonne fréquence de contrats ; que cette utilisation permettrait également de quantifier le recours par les mêmes entreprises aux mêmes intérimaires pour les mêmes types de mission ;

Considérant enfin que l'utilisation du NIR permettrait de suivre la stratégie des intérimaires dans leurs relations avec les entreprises de travail temporaire ;

Considérant que l'utilisation de ce numéro consistera à attribuer les différentes missions effectuées à l'intérimaire en cause ;

Considérant que, hormis dans le cas de l'enquête sur le devenir des intérimaires où le fichier de l'échantillon sera croisé avec le fichier de l'UNEDIC afin de recueillir les nom et adresses des personnes susceptibles d'être enquêtées, il ne sera fait aucun rapprochement avec aucun autre fichier de

quelque provenance que ce soit ; que toute modification de cette utilisation devra faire l'objet d'un examen spécifique par la Commission ;

Considérant que la DARES est un service statistique ministériel dont l'activité de production d'informations statistiques est encadrée par le décret du 17 juillet 1984 portant application de la loi de 1951 modifiée en 1986 relative à l'information, la coordination et au secret en matière de statistiques ;

Emet un **avis favorable** au projet de décret en Conseil d'Etat présenté par ministère de l'emploi et de la solidarité en application de l'article 18 de la loi du 6 janvier 1978.

Délibération n° 99-012 du 9 mars 1999 portant avis sur le projet d'acte réglementaire présenté par le Conseil général de l'Ain et concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer l'aide sociale générale (ANIS-ASG)

La Commission nationale de l'informatique et des libertés,

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 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 pris pour son application ;

Vu la délibération n° 97-091 du 25 novembre 1997 portant avis sur la demande présentée par le Conseil Général de l'Ain et concernant la gestion informatisée de l'aide sociale et de l'action sociale de terrain ;

Vu la délibération n° 98-094 du 13 octobre 1998 concernant les suites à donner à la mission de vérification effectuée les 26 juin et 21 juillet 1998 auprès du Conseil Général de l'Ain et relative à la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer l'aide sociale à l'enfance et l'action sociale de terrain (ANIS-ASE) ;

Vu le projet d'acte réglementaire présenté par le Conseil Général de l'Ain ;

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

Considérant que le Conseil Général de l'Ain a saisi la Commission d'une demande d'avis relative à l'informatisation de la gestion administrative des procédures d'aide sociale générale ; que ce traitement automatisé d'informations nominatives intitulé « ANIS-ASG » assure, à titre principal, la gestion des missions du Conseil Général de l'Ain en matière d'aide sociale générale, à savoir la mise en œuvre et la gestion des procédures d'attribution des prestations d'aide sociale générale, la gestion des informations relatives aux usagers des services départementaux de la Direction de la Prévention et de l'Action Sociale, et la gestion comptable et financière du service d'aide sociale générale ;

Considérant que ce traitement consiste en une base de données unique mise à la disposition, dans la limite de leur habilitation, des agents départementaux affectés aux missions d'aide et d'action sociales du Conseil Général de l'Ain ;

Considérant que les informations enregistrées sont relatives à l'identification des demandeurs ou des bénéficiaires des prestations du service de l'aide sociale générale, à la composition de leur famille et à leur situation économique et financière et à l'état des procédures en cours ;

Considérant que les données relatives aux procédures d'aide sociale générale ne sont pas conservées au-delà de vingt-quatre mois après la date de fin d'effet de la dernière prestation accordée ; que les données nominatives concernant la ou les personnes du dossier familial sont supprimées dès lors qu'aucune procédure n'est en cours et au terme des délais précités ;

Considérant que les informations telles qu'elles résultent des différentes ru briques du traitement ne devront être enregistrées que dans les strictes limites des besoins du travail poursuivi et à la seule initiative du personnel concerné ;

Considérant que seuls auront accès au traitement, dans la limite de leurs attributions et suivant une procédure d'habilitation particulière, les agents départementaux affectés aux services de la Direction de la Prévention et de l'Action Sociale du Conseil Général de l'Ain et participant aux missions d'aide sociale générale ;

Considérant qu'il convient de recommander que des moyens informatiques suffisants soient mis à la disposition de l'ensemble du personnel des services sociaux en particulier des travailleurs sociaux afin qu'ils puissent accéder de façon effective aux dossiers pour lesquels ils sont habilités ; qu'en outre les procédures d'habilitation doivent être définies en concertation avec les personnels des services sociaux concernés et avec le comité de veille ;

Considérant que des mesures de sécurité ont été prévues, notamment pour assurer un accès différencié aux informations selon les habilitations des agents, sous forme de codes d'identification et d'autorisations personnalisées ;

Considérant que, suite aux recommandations formulées par la Commission lors de sa délibération du 13 octobre 1998, le Conseil général de l'Ain a fait part à la Commission des dispositions techniques envisagées :
— pour n'autoriser la recherche d'un dossier, dans la base, qu'après saisie préalable d'au moins les trois premières lettres du nom ;
— pour mettre en place une procédure complémentaire d'analyse des connexions afin de détecter plus efficacement les tentatives d'accès frauduleux à l'application ;
— pour améliorer la procédure de maintenance et éviter tout accès incontrôlé à la base ;

Considérant que ces propositions sont satisfaisantes ; qu'il convient toutefois d'examiner la possibilité de compléter la procédure d'analyse des connexions par un dispositif permettant à des fins de sécurité de conserver, par dossier, une trace temporaire des transactions (saisie, mise à jour et consultation) effectuées ; qu'il convient également de recommander la mise en place soit d'une télémaintenance sur base fictive, soit d'une maintenance sur site, sous le contrôle du responsable informatique du Conseil Général de l'Ain ;

Considérant que le droit d'accès et de rectification des personnes intéressées s'exerce soit directement auprès du centre médico-social pour les informations visualisables par les agents habilités à ce niveau, soit auprès de chaque responsable de circonscription d'action sociale compétente ;

Considérant que toutes dispositions doivent être prises afin d'informer clairement les usagers des destinataires des informations et des droits qui leur sont ouverts au titre de la loi du 6 janvier 1978 et notamment de leur droit d'opposition à la communication des données les concernant aux agents habilités d'autres services sociaux du département ; qu'il convient de recommander à cette fin que les usagers puissent recevoir copie des informations les concernant et que des moyens techniques soient mis en œuvre afin de permettre au travailleur social chargé du suivi du dossier de régler sur demande de l'usager l'accès aux informations de son dossier par d'autres services sociaux ;

Emet un **avis favorable** au projet d'arrêté présenté par le Président du Conseil Général de l'Ain concernant la mise en œuvre d'un traitement automatisé d'informations nominatives relatif à la gestion de l'aide sociale générale.

Délibération n° 99-018 du 25 mars 1999 — portant autorisation d'une enquête épidémiologique présentée par l'INSERM ayant pour finalité d'identifier et de suivre une cohorte d'enfants nés dans le canton de Beaumont-la-Hague entre 1953 et 1997 et ayant été scolarisés entre 1956 et 1997 afin de rechercher une éventuelle surincidence de leucémies et d'étudier la prévalence de malformations congénitales et — portant avis sur un projet d'arrêté présenté par le secrétaire d'État à la santé et à l'action sociale autorisant l'INSERM à utiliser le répertoire national inter-régimes des bénéficiaires de l'assurance maladie

(Demande d'autorisation nº 998166)

La Commission nationale de l'informatique et des libertés,

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 traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la Convention nº 108 du Conseil de l'Europe du 28 janvier 1981 ;

Vu le code de la sécurité sociale, notamment ses articles L 161-32 et R 161-37 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'Informatique, aux fichiers et aux libertés ;

Vu le décret nº 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 ;

Vu le décret nº 98-88 du 18 février 1998 autorisant l'accès aux données relatives au décès des personnes inscrites au répertoire national d'identifica-

tion des personnes physiques dans le cadre des recherches dans le domaine de la santé ;

Vu l'avis rendu le 4 décembre 1998 par le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ;

Vu le projet d'arrêté présenté par le Secrétaire d'Etat à la santé et à l'action sociale ;

Vu la demande d'autorisation présentée par l'INSERM ;

Après avoir entendu Monsieur Jean-Marie POIRIER en son rapport, et Madame Charlotte-Marie PITRAT en ses observations ;

Considérant que l'INSERM (unité 292) saisit la Commission nationale de l'informatique et des libertés d'une demande d'autorisation ayant pour objet de mener une enquête épidémiologique sur l'incidence de leucémies et de cancers de l'enfant et la prévalence de malformations congénitales dans la population des enfants ayant vécu dans le canton de Beaumont-La-Hague à partir de 1966, date de mise en service de l'usine de retraitement de déchets nucléaires ; que cette enquête de cohorte, qui se justifie par l'absence de données scientifiques fiables concernant les éventuels effets sur la santé des personnes de la proximité d'une telle usine, nécessite le recueil de données auprès de sources diverses ;

Considérant que les chercheurs de l'unité 292 de l'INSERM, consulteront, après accord du procureur de la République, les registres d'état civil des dix-neuf communes du canton de Beaumont-La-Hague pour répertorier les enfants nés entre le 1er janvier 1953 et le 31 décembre 1997 d'une mère domiciliée dans le canton de Beaumont-La-Hague à la naissance de l'enfant ; qu'il sera ainsi procédé au recueil de leurs nom, prénoms, sexe, date et lieu de naissance ainsi que de l'adresse des parents ; qu'un rapprochement de ces informations sera ensuite effectué avec les données d'état civil recueillies auprès des registres manuels des écoles, après accord de l'inspecteur d'académie, et des crèches du canton pour les enfants de trois mois à quinze ans ayant fréquenté ces établissements entre le 1er janvier 1953 et le 31 décembre 1997 ;

Considérant que l'unité 292 de l'INSERM pourra, à partir des données ainsi recueillies, rechercher le décès éventuel des personnes en recourant aux services de l'INSEE et de l'INSERM, conformément aux dispositions du décret du 18 février 1998 autorisant l'accès aux données relatives au décès des personnes inscrites au répertoire national d'identification des personnes physiques dans le cadre des recherches dans le domaine de la santé ;

Considérant que, s'agissant des personnes dont on n'aura pas pu retrouver l'adresse, le Secrétaire d'Etat à la Santé et à l'action sociale a estimé, conformément aux dispositions du cinquième paragraphe de l'article R 161-37 du code de la sécurité sociale, que l'intérêt de santé publique justifiait que l'INSERM utilise le répertoire national inter-régimes des bénéficiaires de l'assurance maladie ; qu'ainsi, il présente à la CNIL un projet d'arrêté prévoyant que l'INSERM communiquera à un service particulier de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) les informations suivantes, nécessaires pour interroger le répertoire géré par la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) : nom patronymique, prénoms, année et mois de naissance ou date de naissance, département de naissance ou lieu de naissance, code « commune » INSEE du lieu de naissance, sexe ; que ces informations permettront à la

CNAVTS de communiquer à la CNAMTS les coordonnées des organismes de protection sociale dont relève la personne, à charge pour la CNAMTS, après avoir interrogé les organismes servant les prestations d'assurance maladie de transmettre à l'INSERM les adresses des personnes concernées ;

Considérant que les personnes se verront alors adresser un questionnaire de santé qui comportera plusieurs rubriques relatives respectivement, à l'état civil, à des données socio-démographiques et au suivi médical ; que seront ainsi recueillies des informations sur les différents lieux de résidence et les habitudes de vie et de consommation comme la fréquentation des plages durant l'enfance et la consommation de poissons et coquillages d'origine locale pendant la grossesse ; que s'agissant du suivi médical de la personne, seront recueillies des données sur la survenue d'une ou plusieurs pathologies étudiées et des renseignements permettant de valider le diagnostic ; qu'à cet effet seront collectées les coordonnées des médecins traitants et hospitaliers et des maternités afin de permettre à l'INSERM, avec l'autorisation écrite des personnes concernées de contacter, le cas échéant, ces médecins ;

Considérant que l'exploitation statistique des données figurant sur le questionnaire renvoyé sous enveloppe « T » à l'INSERM, permettra d'avoir des informations sur les diagnostics de cancer, leucémie ou malformation congénitale, date des premiers symptômes ou de la première hospitalisation, date de diagnostic, siège de la tumeur ou de la malformation, classification des leucémies, cancers ou malformations congénitales diagnostiqués, caractéristiques histologiques, malignité, commune de résidence lors du diagnostic ;

Considérant que l'information des personnes concernées, telle qu'elle est prévue par l'article 40-5 de la loi du 6 janvier 1978 modifiée sera assurée par la lettre accompagnant le questionnaire ;

Considérant que la sécurité du fichier constitué à l'INSERM sera assurée notamment, par une séparation physique des supports comportant les données d'identification et les données médicales ;

Autorise la mise en œuvre par l'unité 292 de l'INSERM du traitement ayant pour finalité d'identifier et de suivre une cohorte d'enfants nés dans le canton de Beaumont-La-Hague entre 1953 et 1997 et ayant été scolarisés entre 1956 et 1997 afin de rechercher une éventuelle surincidence de leucémies et d'étudier la prévalence de malformations congénitales,

Emet un **avis favorable** au projet d'arrêté présenté par le Secrétaire d'Etat à la santé et à l'action sociale autorisant l'utilisation par l'unité 292 de l'INSERM du répertoire national inter-régimes des bénéficiaires de l'assurance maladie sous les réserves suivantes :

— dans le titre de l'arrêté, substituer aux mots « à des fins de recherche des personnes » les mots « à des fins d'identification des organismes servant les prestations d'assurance maladie aux personnes devant être interrogées dans le cadre d'une enquête épidémiologique »,

— à l'article 1er, remplacer les mots « par l'enquête... modalités appropriées de suivi médical » par les mots « par l'enquête relative aux risques éventuels liés à la proximité d'installations de stockage et de retraitement de matières nucléaires de La Hague ».

Délibération n° 99-019 du 25 mars 1999 relative à la transmission d'informations fiscales par la Direction générale des impôts à divers organismes de sécurité sociale et aux services des pensions de la Direction générale de la comptabilité publique

(Demande d'avis modificative n° 104 337)

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 relative à l'informatique, aux fichiers et aux libertés, ainsi que son décret d'application n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu le livre des procédures fiscales, notamment ses articles L. 103, L. 113 ainsi que l'article L. 152 dans sa rédaction issue de la loi de finances pour 1999 ;

Vu le code général des impôts, notamment ses articles 1417-I bis et 1657-1 bis ;

Vu la loi n° 96-1160 du 27 décembre 1996 de financement de la sécurité sociale pour 1997 ;

Vu l'arrêté du 28 avril 1987 relatif à la création d'un traitement informatisé de simplification de la gestion des informations de recoupement (traitement « SIR »), modifié par les arrêtés du 31 janvier 1989, du 19 avril 1995, du 4 décembre 1996, du 18 février 1997, du 4 août 1997, du 21 janvier 1998 et du 14 avril 1998 ;

Vu les délibérations de la CNIL n° 95-026 et 95-027 du 7 mars 1995 ;

Vu le projet d'arrêté modifiant l'arrêté du 28 avril 1987 présenté par le ministère de l'économie, des finances et de l'industrie ;

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, des finances et de l'industrie a saisi la Commission d'une demande d'avis modificative relative à l'application dénommée « SIR » de la direction générale des impôts (DGI), dont la finalité principale est d'assurer la collecte des informations de recoupement communiquées à l'administration fiscale par les organismes tiers-payeurs, ainsi que leur exploitation par rapprochement avec les déclarations fiscales de revenus des contribuables ;

Considérant que la modification envisagée a pour objet, d'une part, de réviser la liste des catégories d'informations fiscales transmises sur support informatique, respectivement à la caisse nationale des allocations familiales (CNAF) et à la caisse nationale d'assurance vieillesse des travailleurs salariés (CNAV), d'autre part, d'autoriser de nouveaux transferts d'informations au bénéfice de la caisse centrale de la mutualités sociale agricole (CCMSA) et de la direction générale de la comptabilité publique (DGCP) ;

Considérant que les circuits d'informations envisagés doivent être conformes à l'article L. 152 du livre des procédures fiscales, qui dispose, dans le dernier état de rédaction résultant de la loi de finances pour 1999, que des circuits d'informations peuvent être mis en place par l'administration fiscale, afin de communiquer aux organismes et services chargés de la gestion d'un

régime obligatoire de sécurité sociale ainsi qu'aux institutions de retraite complémentaire, les informations nominatives nécessaires :

1° A l'appréciation des conditions d'ouverture et de maintien des droits aux prestations ;

2° Au calcul des prestations ;

3° A l'appréciation des conditions d'assujettissement aux cotisations et contributions ;

4° A la détermination de l'assiette et du montant des cotisations et contributions ainsi qu'à leur recouvrement ;

Sur la transmission d'informations à la CNAF

Considérant que la CNAF reçoit chaque année, depuis 1995, des informations issues des déclarations fiscales de revenus de l'ensemble des personnes — allocataires, conjoints, personnes à charge — dont les ressources sont prises en compte pour l'attribution des prestations versées sous condition de ressources, afin de permettre le contrôle des déclarations annuelles ou trimestrielles de ressources adressées par les allocataires aux caisses d'allocations familiales ;

Considérant que si la DGI prévoit la transmission des informations relatives aux revenus de l'année N-2, dans l'hypothèse où aucun élément de taxation ne serait disponible pour l'année N-1, la CNAF a, dans les derniers jours de l'instruction du dossier, informé la Commission de l'abandon de ce projet qui ne répondait pas à ses attentes initiales ; que, dès lors, les informations qui restent transmises à la CNAF sont adéquates, pertinentes et non excessives pour l'appréciation des conditions d'ouverture et de maintien des droits aux prestations soumises à condition de ressources et pour la vérification du calcul des prestations différentielles ;

Considérant, par ailleurs, qu'indépendamment de l'information assurée par les organismes de sécurité sociale destinataires des informations, les contribuables sont informés par la DGI de la transmission aux caisses d'allocations familiales d'informations issues de la déclaration de revenus n° 2042 des personnes dont les revenus sont pris en compte pour l'attribution de prestations versées sous condition de ressources ;

Sur la transmission d'informations à la CNAV

Considérant que la CNAV reçoit chaque année, depuis 1995, des informations concernant la situation fiscale des pensionnés du régime général, afin de permettre le calcul du montant de la contribution sociale généralisée (CSG) et de la cotisation d'assurance maladie, qui doivent être prélevées à la source par les organismes payeurs sur le montant des pensions de retraite ;

Considérant en effet que sont exonérées de ces prélèvements obligatoires les pensions versées l'année N à des personnes qui bénéficiaient d'une mesure d'exonération ou d'exemption au titre de l'impôt sur le revenu dû l'année N-1 ; qu'en outre, le taux de cotisation applicable est fonction du revenu fiscal de référence, qui est calculé avant prise en compte des éventuels crédits d'impôts ;

Considérant que les catégories d'informations transmises à la CNAV se limitent, à compter de cette année, à un code « imposable » ou « non imposable » au regard de l'article 1657-1 bis du code général des impôts, et à un code « imposable » ou « non imposable » au regard de l'article 1417-I bis du CGI ; qu'en outre, dans l'hypothèse où aucun élément ne serait disponible au titre de l'année N-1, il est prévu de restituer les éléments fiscaux se

rapportant à l'année précédente ; que ces informations sont adéquates, pertinentes et non excessives pour apprécier les conditions d'assujettissement aux cotisations et contributions et en déterminer le montant ;

Considérant, par ailleurs, qu'indépendamment de l'information assurée par les organismes de sécurité sociale destinataires des informations, les contribuables sont informés par la DGI de la transmission aux organismes gestionnaires des retraites du régime général de sécurité sociale d'informations issues du traitement des déclarations fiscales de revenus des personnes auxquelles ils versent une pension de retraite ;

Sur la transmission d'informations à la CCMSA

Considérant que la CCMSA souhaite obtenir de la DGI, à l'instar des échanges équivalents mis en place avec la CNAV, les informations nécessaires à la détermination du taux d'appel de la CSG qui est applicable aux pensions d'invalidité ou de retraite versées par le régime agricole ;

Considérant que les informations communiquées par la DGI sont identiques à celles déjà qui sont transmises à la CNAV ; qu'à cette fin, la CCMSA constitue un fichier national d'appel, comportant, pour chaque pensionné : le nom, les prénoms, les date et lieu de naissance, le code sexe, l'adresse au 31 décembre et un numéro d'ordre annuel ;

Considérant qu'en sus des mesures d'information qui sont à la charge des caisses de la mutualité sociale agricole, les contribuables doivent être informés au moment de la collecte des données, c'est-à-dire sur les déclarations fiscales de revenus, de la liste des organismes tiers qui sont habilités à recevoir communication de tout ou partie des renseignements recueillis ou issus de leur exploitation ;

Mais considérant qu'il y a lieu, au cas particulier, de tenir compte de l'intérêt du dispositif pour les pensionnés, eu égard à la simplification des procédures administratives qui leur étaient jusque là applicables, les échanges automatisés envisagés devant dispenser les intéressés d'être obligées d'adresser leur avis d'imposition à leur caisse de mutualité sociale agricole ;

Considérant qu'il convient cependant que les prochains formulaires de déclaration fiscale de revenus soient complétés afin de mentionner l'existence de ces nouveaux transferts d'informations ;

Considérant, par ailleurs, que les informations issues des fichiers de la DGI ne seront transmises qu'en cas de concordance absolue des éléments d'identification fournies par la CCMSA avec ceux détenus par la DGI ;

Considérant, enfin, que les informations reçues par la DGI seront détruites à l'issue des opérations de transfert et qu'elles ne feront l'objet d'aucune exploitation à des fins fiscales ;

Sur la transmission d'informations à la DGCP

Considérant que la DGCP souhaite mettre en place avec la DGI le même circuit d'informations que celui décrit ci-dessus, afin de permettre à ses centres régionaux des pensions de procéder au prélèvement à la source de la CSG et d'appliquer les mesures d'exonération totale ou partielle des prélèvements fiscaux à affectation sociale, sans être pour autant obligés de demander au préalable chaque année à l'ensemble des retraités de l'Etat une copie de leur avis d'imposition ou de non-imposition ;

Considérant que le fichier d'appel de la DGCP comprend les nom et prénoms, le sexe, les date et lieu de naissance, l'adresse et un numéro de liaison

formé à partir du numéro de pension et des dix premiers caractères du numéro de sécurité sociale ;

Considérant que les conditions de transmission et d'exploitation des informations ne se distinguent pas de celles applicables dans le cadre des échanges avec la CNAV et la CCMSA et que les mesures d'informations à la charge de la DGI doivent être organisées dans les mêmes conditions que pour les transferts de données fiscales susmentionnés ;

Considérant en outre, d'une part, que le principe d'égalité de traitement devant les charges publiques s'oppose à toute rupture d'égalité injustifiée entre les pensionnés qui résulterait de la nature de la pension de retraite qui leur est servie, d'autre part, que le dispositif proposé constitue une mesure de simplification administrative bénéficiant directement aux personnes concernées ;

Considérant cependant qu'il ne saurait être fait application à la DGCP de l'article L. 152 modifié du livre des procédures fiscales qui ne prévoit de communication d'informations par la DGI qu'au bénéfice des organismes et services chargés de la gestion d'un régime obligatoire de sécurité sociale et des institutions de retraite complémentaire ; que la DGCP, qui applique les dispositions du code des pensions civiles et militaires de retraite, n'entre pas dans le champ d'application de cette disposition puisqu'elle ne répond à aucun de ses critères ; qu'ainsi et jusqu'à nouvelle modification de l'article L. 152 du LPF à cette fin, la transmission envisagée est légalement impossible ;

Emet, sous le bénéfice des observations qui précèdent, un **avis favorable** sur le projet d'acte réglementaire modifiant l'arrêté du 28 avril 1987, présenté par le ministère de l'économie des finances et de l'industrie, sous réserve :
— de la suppression du paragraphe consacré aux agents habilités des centres régionaux des pensions des services déconcentrés du Trésor Public,
— de la suppression, à l'alinéa 2 du nouvel article 7, des mots « ou, à défaut, pour l'année N-2 »,
— de la modification comme suit du dernier alinéa du nouvel article 7 :
« les informations transmises pour la détermination des taux de cotisations sont, pour l'année N-1 ou, à défaut, pour l'année N-2, les suivantes : (la suite sans changement) »,

Demande au ministère chargé du budget de veiller à ce qu'une disposition soit ajoutée à l'article L. 152 du livre des procédures fiscales, ou dans telle autre disposition qu'il paraîtrait opportun de modifier, afin qu'une dérogation à la règle du secret professionnel puisse être légalement instituée au profit des centres des pensions de la DGCP pour ce qui concerne les informations nécessaires à l'appréciation des conditions d'assujettissement aux contributions et au calcul de leur montant.

Délibération n° 99-020 du 25 mars 1999 concernant la transmission aux caisses de la mutualité sociale agricole d'informations relatives à la situation fiscale des bénéficiaires d'une pension de retraite ou d'invalidité

(Demande d'avis nº 637 394)

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que son décret d'application nº 78-774 du 17 juillet 1978 ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu le code de la sécurité sociale, notamment son article L. 136-5 II ;

Vu le livre des procédures fiscales, notamment ses articles L. 103, L. 113, ainsi que l'article L. 152 dans sa rédaction issue de la loi de finances pour 1999 ;

Vu le code général des impôts, notamment ses articles 1417-I bis et 1657-1 bis ;

Vu le projet d'acte réglementaire de la caisse centrale de la mutualité sociale agricole ;

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

Considérant que la caisse centrale de la mutualité sociale agricole (CCMSA) a saisi la Commission d'une demande d'avis relative à la mise en place d'un traitement automatisé d'échange d'informations nominatives entre la direction générale des impôts (DGI) et les organismes chargés du paiement des pensions de retraite et d'invalidité du régime agricole (MSA) ;

Considérant que sont exonérées de la cotisation sociale généralisée (CSG), prélèvement fiscal à affectation sociale, les pensions versées l'année N à des personnes bénéficiant d'une mesure d'exonération ou d'exemption d'impôt sur le revenu au titre de l'impôt dû en N-1 et que le taux de cotisation applicable à la CSG est fonction du revenu fiscal de référence qui est calculé avant prise en compte des éventuels crédits d'impôts ; que, dans ce contexte, le traitement a pour finalité la transmission annuelle, aux caisses locales de la MSA, de la situation fiscale des pensionnés au regard de l'impôt sur le revenu, afin de calculer le montant de la CSG due sur les pensions et de procéder à son prélèvement à la source ;

Considérant que la CCMSA adresse à la DGI un fichier national d'appel comportant, pour chaque pensionné, les catégories d'informations suivantes : le nom, les prénoms, les date et lieu de naissance, le code sexe, l'adresse au 31 décembre, un numéro d'ordre annuel ; que la transmission de ce fichier à la DGI doit permettre la consultation du fichier des impositions à l'impôt sur le revenu et la constitution sur bandes magnétiques d'un fichier décrivant la situation fiscale des pensionnés ;

Considérant que les catégories d'informations transmises aux caisses de la MSA, par l'intermédiaire de la CCMSA, sont un code « imposable » ou « non imposable » au regard de l'article 1657-1 bis du code général des impôts et un code « imposable » ou « non imposable » au regard de l'article 1417-I bis du CGI ; que les informations ne sont retournées par la DGI qu'en cas d'identité parfaite entre les éléments communiqués par la DGCP et ceux détenus par la DGI ; que dans l'hypothèse où aucun élément ne serait disponible au titre de l'année N-1, il est prévu de restituer les éléments fiscaux relatifs à l'année précédente ; que ces informations sont adéquates, pertinentes et non excessives pour apprécier les conditions d'assujettissement à la CSG et en déterminer le montant ;

Considérant qu'indépendamment de l'information assurée par la DGI, les décomptes trimestriels de pension adressés par les caisses de MSA doivent informer chaque année les pensionnés de la réception d'informations issues du traitement des déclarations fiscales de revenus afin de connaître le taux

d'appel de la CSG et que ces courriers doivent également comporter un rappel des droits d'accès et de rectification ;

Emet un **avis favorable** sur le projet d'acte réglementaire de la CCMSA.

Délibération n° 99-021 du 25 mars 1999 concernant la transmission aux centres régionaux des pensions de la Direction générale de la comptabilité publique d'informations relatives à la situation fiscale des bénéficiaires d'une pension de retraite

(Demande d'avis modificative n° 62152)

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 relative à l'informatique, aux fichiers et aux libertés, ainsi que son décret d'application n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu le code général des impôts, notamment ses articles 1417-I bis et 1657-1 bis ;

Vu le livre des procédures fiscales, notamment ses articles L. 103, L. 113 ainsi que l'article L. 152 dans sa rédaction issue de la loi de finances pour 1999 ;

Vu le code des pensions civiles et militaires de retraite ;

Vu la loi n° 96-1160 du 27 décembre 1996 de financement de la sécurité sociale pour 1997 ;

Vu le décret n° 62-1587 du 26 décembre 1962 portant règlement général sur la comptabilité publique ;

Vu l'arrêté du 21 janvier 1992 portant création d'un traitement automatisé des pensions de l'Etat et émoluments divers (traitement « PEZ ») ;

Vu le projet d'arrêté du secrétaire d'Etat au budget modifiant l'arrêté du 21 janvier 1992 ;

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

Considérant que la demande d'avis modificative formée auprès de la Commission par la direction générale de la comptabilité publique (DGCP) porte sur le traitement « PEZ », qui a pour finalité principale la gestion et le paiement des pensions civiles et militaires de l'Etat, des pensions militaires d'invalidité et de victime de guerre et des émoluments assimilés ;

Considérant que sont exonérées de la contribution sociale généralisée (CSG), prélèvement fiscal à affectation sociale, les pensions versées l'année N à des personnes bénéficiant d'une mesure d'exonération ou d'exemption d'impôt sur le revenu au titre de l'impôt dû en N-1 et que le taux de cotisation applicable à la CSG est fonction du revenu fiscal de référence qui est calculé avant prise en compte des éventuels crédits d'impôts ; que, dans ce contexte, la principale modification envisagée a pour finalité la transmission annuelle par la direction générale des impôts (DGI) aux centres régionaux des pensions de la DGCP de la situation fiscale des bénéficiaires d'une pension de retraite au regard de l'impôt sur le revenu, afin de calculer le mon-

tant de la CSG due sur les pensions et de procéder à son prélèvement à la source ;

Considérant que le fichier d'appel transmis par la DGCP comprendrait les nom et prénom, le sexe, les date et lieu de naissance, l'adresse et un numéro de liaison formé à partir du numéro de pension et des dix premiers caractères du NIR ; que la transmission de ce fichier à la DGI devrait permettre la consultation du fichier des impositions à l'impôt sur le revenu et la constitution sur bandes magnétiques d'un fichier décrivant la situation fiscale des pensionnés ;

Considérant que les catégories d'informations transmises à la DGCP seraient un code « imposable » ou « non imposable » au regard de l'article 1657-1 bis du CGI et un code « imposable » ou « non imposable » au regard de l'article 1417-I bis CGI ; que dans l'hypothèse où aucun élément ne serait disponible au titre de l'année N-1, il est prévu de restituer les éléments fiscaux relatifs à l'année précédente ; que ces informations sont adéquates, pertinentes et non excessives pour apprécier les conditions d'assujettissement à la CSG et en déterminer le montant ;

Considérant que les informations ne seraient retournées par la DGI qu'en cas d'identité parfaite entre les éléments communiqués par la DGCP et ceux détenus par la DGI ; qu'à défaut, le traitement continuerait à être effectué manuellement en interrogeant le pensionné ;

Considérant, d'une part, que le principe d'égalité de traitement devant les charges publiques s'oppose à toute rupture d'égalité injustifiée entre les pensionnés qui résulterait de la nature de la pension de retraite qui leur est servie, d'autre part, que le dispositif proposé constitue une mesure de simplification administrative bénéficiant directement aux personnes concernées ;

Considérant cependant qu'il ne saurait être fait application à la DGCP de l'article L. 152 modifié du livre des procédures fiscales qui ne prévoit de communication d'informations par la DGI qu'au bénéfice des organismes et services chargés de la gestion d'un régime obligatoire de sécurité sociale et des institutions de retraite complémentaire ; que la DGCP, qui applique les dispositions du code des pensions civiles et militaires de retraite, n'entre pas dans le champ d'application de cette disposition puisqu'elle ne répond à aucun de ses critères ; qu'ainsi et jusqu'à nouvelle modification à cette fin de l'article L. 152 du LPF, la transmission envisagée est légalement impossible ;

Considérant que les autres dispositions du projet d'arrêté, qui portent sur la liste des organismes destinataires des informations traitées dans le cadre du traitement « PEZ » ainsi que sur la non-application audit traitement du droit d'opposition de l'article 26 de la loi du 6 janvier 1978, n'appellent pas d'observation particulière ;

Emet un **avis favorable** sur le projet d'arrêté modificatif du secrétaire d'Etat au budget, sous réserve de la suppression de l'article 2 relatif aux échanges de données entre la DGI et la DGCP,

Demande au ministère chargé du budget de veiller à ce qu'une disposition soit ajoutée à l'article L. 152 du livre des procédures fiscales, ou dans telle autre disposition qu'il paraîtrait opportun de modifier, afin qu'une dérogation à la règle du secret professionnel puisse être légalement instituée au profit des centres des pensions de la DGCP pour ce qui concerne les informations nécessaires à l'appréciation des conditions d'assujettissement aux contributions et au calcul de leur montant.

Délibération n° 99-023 du 8 avril 1999 portant avis sur le projet d'arrêté concernant la création par le ministère de l'Intérieur d'un traitement automatisé d'informations nominatives relatif à la délivrance des passeports (application « DELPHINE »)

La Commission nationale de l'informatique et des libertés,

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

Vu le code pénal ;

Vu le code de procédure pénale, et notamment son article 78-2 ;

Vu le décret modifié n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII de la loi du 6 janvier 1978 ;

Vu l'arrêté du 15 mai 1996 relatif au fichier des personnes recherchées géré par le ministère de l'intérieur et le ministère de la défense ;

Vu les délibérations n° 88-120 du 8 novembre 1988 et n° 92-56 du 9 juin 1992 portant avis sur le projet d'arrêté relatif au fichier des personnes recherchées géré par le ministère de l'intérieur et le ministère de la défense ;

Vu le projet d'arrêté interministériel portant création par le ministère de l'intérieur du traitement automatisé d'informations nominatives relatif à la délivrance des passeports ;

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

Considérant que la Commission est saisie par le ministère de l'intérieur d'un projet d'arrêté interministériel portant création d'un traitement automatisé d'informations nominatives relatif à la délivrance des passeports ;

Considérant que le projet du ministère de l'intérieur a pour objet de créer un système de fabrication et de gestion informatisé des passeports et un fichier national des passeports en cours de validité ; que ce système devrait permettre de limiter les risques de falsification ou de contrefaçon des titres ;

Considérant que le traitement sera progressivement mis en place au sein des services du ministère de l'intérieur et du ministère des affaires étrangères chargés de la délivrance des passeports, principalement les préfectures et sous-préfectures, la préfecture de police de Paris, les postes diplomatiques pourvus d'une section consulaire et les postes consulaires à l'étranger ;

Considérant que la délivrance des passeports sera systématiquement précédée de la consultation du fichier des personnes recherchées ; qu'il appartient au ministère de l'intérieur de rappeler aux agents des services chargés de la délivrance des passeports de respecter scrupuleusement les conduites à tenir dans l'hypothèse où le demandeur du titre fait l'objet d'une inscription au fichier des personnes recherchées, comme l'ont prévu les délibérations n° 88-120 du 8 novembre 1988 et n° 92-56 du 9 juin 1992 concernant le fichier des personnes recherchées ;

Considérant que les informations enregistrées dans le traitement concerneront l'identité du demandeur (nom patronymique ou nom d'usage, pseudonyme, surnom, prénoms, prénom usuel, date et lieu de naissance), son signalement (sexe, couleur des yeux, taille), son adresse et, à la demande de

l'intéressé, sa profession, le nombre et l'identité des enfants inscrits sur le passeport ; qu'en outre, le traitement comportera des informations relatives à l'autorité qui délivre le passeport (identifiant des agents qui participent à la production du titre) et au passeport délivré (numéro, type de passeport, fiscalité, date et lieu de délivrance, date d'expiration, type et date d'événement affectant le passeport (perte, vol, destruction, annulation), mentions de justificatifs liés à la délivrance du passeport, date d'expiration) ; qu'enfin, des données relatives à la demande de passeport seront saisies dans le traitement ; qu'il s'agira du numéro de demande, du lieu de dépôt, de la date de réception de demande, de la date d'envoi du titre au guichet de dépôt et du motif de non délivrance de passeport ;

Considérant que ces informations sont adéquates, pertinentes, et non excessives au regard de la finalité du traitement ;

Considérant que le passeport comportera une zone de lecture optique ; qu'il résulte du dossier transmis par le ministère de l'intérieur à l'appui du projet d'arrêté portant création du traitement que cette zone de lecture fera état du nom, des prénoms, du sexe, de la date de naissance et de la nationalité du titulaire, du type de document, du numéro de passeport et de la date d'expiration du titre ; que le projet d'arrêté devra énumérer ces informations ; qu'en outre, il devra expressément indiquer que cette zone de lecture ne pourra être utilisée pour mettre en mémoire des informations mentionnées sur le passeport, modifier les données existantes dans la base nationale ou accéder à tout autre fichier ;

Considérant que les modalités d'acquisition de la nationalité française, la filiation et, le cas échéant, le numéro de la carte nationale d'identité sécurisée dont est titulaire le demandeur d'un passeport, informations recueillies à l'occasion d'une demande de délivrance de passeport, ne seront pas enregistrés dans le traitement ;

Considérant que les critères d'interrogation du fichier national des passeports délivrés seront le numéro de série, le numéro de formulaire de demande et l'état-civil du titulaire du passeport (nom, prénom, date de naissance) ;

Considérant que l'article 8 du projet d'arrêté dispose que les données enregistrées dans le traitement ne pourront faire l'objet d'aucune cession ou communication à des tiers ; qu'en outre, il devra être précisé que ces données ne pourront faire l'objet d'aucune interconnexion ;

Considérant que la durée de conservation des informations enregistrées sera de douze ans, conformément à la circulaire interministérielle du 5 juillet 1994 relative au traitement et à la conservation des documents liés à la nationalité, produits dans les préfectures et sous-préfectures ;

Considérant que les destinataires des informations enregistrées seront, en fonction de leurs attributions respectives, les personnels chargés de l'établissement ou du suivi de l'établissement des passeports, de l'application de la réglementation relative aux passeports dans les services centraux du ministère de l'intérieur, des missions de recherche et contrôle de l'identité des personnes, de vérification de la validité et de l'authenticité des passeports au sein des services de la police nationale, de la gendarmerie nationale et des douanes ; que l'article 4 du projet d'arrêté devra préciser que l'accès aux données s'effectuera pour les besoins exclusifs de l'accomplissement de ces missions ;

Considérant que le formulaire de demande de délivrance d'un passeport devra mentionner, conformément à l'article 27 de la loi du 6 janvier 1978, les

personnes physiques ou morales destinataires des informations et l'existence d'un droit d'accès et de rectification ;

Considérant que le droit d'accès aux informations enregistrées s'exercera, en application des dispositions de l'article 34 de la loi du 6 janvier 1978, auprès des services en charge de la délivrance des passeports ; que toutefois, les éventuelles rectifications seront opérées par la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur ;

Considérant que les mesures de sécurité prévues par le ministère de l'intérieur comprendront d'une part, un contrôle de l'accès au traitement au moyen de cartes à puce personnalisées permettant d'identifier chaque utilisateur du traitement, d'autre part, un système de journalisation permettant de connaître l'ensemble des opérations effectuées ;

Emet un **avis favorable** sur le projet d'arrêté interministériel portant création du traitement automatisé d'informations nominatives relatif à la délivrance des passeports, sous réserve que :

— le projet d'arrêté énumère les informations inscrites dans la zone de lecture optique qui figurera sur les passeports ; qu'il précise en outre que cette zone de lecture ne pourra être utilisée pour mettre en mémoire des informations mentionnées sur le passeport, modifier les données existantes dans la base nationale ou accéder à tout autre fichier que le fichier national des passeports en cours de validité ;

— le projet d'arrêté précise que les données enregistrées dans le traitement ne pourront faire l'objet d'aucune interconnexion ;

— l'article 4 du projet d'arrêté précise que l'accès aux données enregistrées s'effectuera pour les besoins exclusifs de l'accomplissement des missions énumérées à ce même article ;

— les formulaires de demande de délivrance d'un passeport mentionnent les personnes physiques ou morales destinataires des données enregistrées ;

Recommande au ministère de l'Intérieur de rappeler aux agents chargés de la délivrance des passeports de respecter scrupuleusement les conduites à tenir lors de la consultation du fichier des personnes recherchées.

Délibération n° 99-025 du 22 avril 1999 portant modification : — de la norme simplifiée n° 36 concernant les traitements automatisés d'informations nominatives relatifs à la liquidation et au paiement des rémunérations des personnels de l'État et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public ; — de la norme simplifiée n° 37 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des personnels de l'État et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public

La Commission nationale de l'informatique et des libertés,

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment ses articles 6, 17 et 21 (1°), pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu les délibérations n° 93-020 et 93-021 du 2 mars 1993 concernant les traitements automatisés d'informations nominatives relatifs à la liquidation et au paiement des rémunérations ainsi qu'à la gestion des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public ;

Considérant qu'il y a lieu d'alléger les formalités préalables à la mise en œuvre des traitements ayant pour finalité la liquidation et le paiement des rémunérations ainsi que la gestion des personnels de l'Etat et de ses établissements publics, des collectivités territoriales et de leurs établissements publics et des personnes morales de droit privé gérant un service public, en supprimant l'obligation de joindre aux déclarations simplifiées de conformité aux normes simplifiées n° 36 et 37, une annexe précisant les dispositions particulières de sécurité ;

Décide :

— le deuxième alinéa de l'article 6 de la norme simplifiée n° 36 est supprimé ;
— le deuxième alinéa de l'article 6 de la norme simplifiée n° 37 est supprimé.

Délibération n° 99-026 du 22 avril 1999 portant modification de la norme simplifiée n° 23 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des membres des associations à but non lucratif régies par la loi du 1er juillet 1901

La Commission nationale de l'informatique et des libertés,

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment ses articles 6, 17 et 21 (1°), pris ensemble le décret n° 78-774 du 17 juillet 1978 ;

Vu la délibération n° 81-89 du 21 juillet 1981 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des membres des associations à but non lucratif régies par la loi du 1er juillet 1901 ;

Considérant qu'il y a lieu d'alléger les formalités préalables à la mise en œuvre des traitements ayant pour finalité la gestion par une association du fichier de ses adhérents en supprimant l'obligation de joindre en annexe au formulaire de déclaration de conformité à la norme la liste des informations recueillies ainsi que l'article des statuts définissant l'objet de l'association et en élargissant le champ d'application du texte aux traitements ayant pour finalité l'édition d'annuaires de membres d'une association ;

Considérant qu'il y a lieu de préciser les catégories d'informations qui sont exclues du bénéfice de la norme simplifiée n° 23 et de rappeler les droits reconnus par la loi du 6 janvier 1978 aux personnes concernées par le traitement ;

Décide :

L'article 2 de la norme simplifiée n° 23 est complété par un alinéa ainsi rédigé :

« c) d'établir des annuaires de membres, à l'exception des annuaires mis à la disposition du public sur le réseau Internet. »

L'article 3 est ainsi rédigé :

« Article 3

Catégories d'informations traitées et droits des personnes concernées

I — Catégories d'informations traitées :

Les informations collectées et traitées doivent être adéquates, pertinentes et non excessives au regard de l'objet de l'association.

Ne peuvent être collectées ni traitées dans le cadre de la présente norme les informations suivantes :
— les informations susceptibles de faire apparaître, directement ou indirectement, les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes (article 31 de la loi du 6 janvier 1978) ;
— les informations concernant les infractions, condamnations ou mesures de sûreté (article 30 de la loi du 6 janvier 1978) ;
— les informations relatives à la santé des personnes concernées ;
— les informations relatives aux difficultés sociales et économiques des personnes ;
— le numéro d'inscription au répertoire d'identification des personnes (n° INSEE ou n° de sécurité sociale) (article 18 de la loi du 6 janvier 1978).

II — Droits des personnes concernées :

L'association s'engage à respecter les dispositions de l'article 27 de la loi du 6 janvier 1978 en informant les personnes, lors de leur adhésion, du caractère obligatoire ou facultatif des informations demandées, des conséquences d'un défaut de réponse, des catégories de destinataires des informations et du lieu où s'exerce le droit d'accès et de rectification.

Lorsque les informations figurent dans un annuaire appelé à être diffusé, les adhérents doivent en être préalablement informés et doivent être mis en mesure de s'opposer à ce que tout ou partie des informations les concernant soient publiées. «

L'article 5 est complété par un dernier alinéa ainsi rédigé :

« En outre, et sous réserve des dispositions de l'article 3 II de la présente norme, les informations relatives aux membres de l'association peuvent faire l'objet d'une diffusion sous la forme d'un annuaire dans les conditions prévues par l'article 2 c). »

L'article 6 est ainsi rédigé :

« Tout traitement dont les caractéristiques ne sont pas conformes aux dispositions précitées doit faire l'objet d'une déclaration ordinaire ou d'une demande d'avis, au moyen, le cas échéant, du formulaire de déclaration spécifique de traitements mis en œuvre dans le cadre d'un site Internet. »

Délibération n° 99-027 du 22 avril 1999 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des prêts de livres, de supports audiovisuels et d'œuvres artistiques et à la gestion des consultations de documents d'archives publiques

(Norme simplifiée n° 9)

La Commission nationale de l'informatique et des libertés,

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

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment ses articles 6, 17 et 21 (1°), pris ensemble le décret nº 78-774 du 17 juillet 1978 ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi nº 80-532 du 15 juillet 1980 relative à la protection des collections publiques contre les actes de malveillance ;

Vu l'article 322-2 du code pénal ;

Vu la délibération nº 80-17 du 6 mai 1980 concernant les traitements automatisés d'informations nominatives relatifs à la gestion de prêts de livres, de supports audiovisuels et d'œuvres artistiques ;

Considérant que la Commission nationale de l'informatique et des libertés est habilitée, en vertu des articles 6, 17 et 21 (1°) à édicter, en vertu de son pouvoir réglementaire, des normes simplifiées concernant certains traitements automatisés d'informations nominatives ;

Considérant que, pour l'application de l'article 17 susvisé, il faut entendre par norme simplifiée l'ensemble des conditions que doivent remplir certaines catégories les plus courantes de traitements pour être regardées comme ne comportant manifestement pas de risques d'atteinte à la vie privée et aux libertés et comme pouvant dès lors faire l'objet d'une déclaration simplifiée ;

Considérant que certains des traitements informatisés portant sur la gestion des prêts de livres, de supports audiovisuels et d'œuvres artistiques sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné ; qu'il en est de même pour la gestion des consultations de documents d'archives publiques ;

Décide :

Article 1er

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée les traitements automatisés d'informations nominatives relatifs aux prêts de livres, de supports audiovisuels et d'œuvres artistiques et à la gestion des consultations de documents d'archives publiques doivent :
— ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès ;
— n'appliquer à ces données que des logiciels dont les résultats puissent être facilement contrôlés ;
— ne pas donner lieu à des interconnexions autres que celles nécessaires à l'accomplissement des fonctions énoncées à l'article 2 ci-dessous ;
— comporter des dispositions propres à assurer la sécurité des traitements et des informations à la garantie des secrets protégés par la loi ;
— satisfaire en outre aux conditions énoncées aux articles 2 à 5 ci-dessous ;
— ne pas déroger aux lois et règlements concernant les droits de propriété, d'auteur, de compositeur et d'interprétation liés aux supports prêtés et à la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Article 2
Finalités des traitements

Les traitements doivent avoir pour seules fonctions :
— de fournir des informations individuelles pour la gestion financière des prêts et la récupération des ouvrages ou supports prêtés ou consultés ;

— d'éditer des états statistiques dépersonnalisés pour les besoins de gestion et d'amélioration des services rendus (nature des ouvrages et des documents d'archives les plus souvent consultés, nom des œuvres et des auteurs ou références des documents d'archives, etc.) ;

Article 3
Catégories d'informations traitées

Dès lors que les dispositions de l'article 27 de la loi nº 78-17 du 6 janvier 1978 ont été respectées lors de leur recueil, les informations traitées doivent seulement relever des catégories suivantes :
— nom, prénoms, adresse, année de naissance, catégorie professionnelle, numéro de téléphone, et, sous forme facultative, la nature de la recherche s'agissant des documents d'archives ;
— caractéristiques du prêt ou de la communication : désignation de l'œuvre (titre, nom de l'auteur, de l'éditeur, etc.) ou du document d'archive, cotes de catalogage ou de classement, date, date (s) de relance.

Article 4
Durée de conservation

Les informations relatives à l'identité des emprunteurs sont conservées tant qu'ils continuent à participer au service de prêts. La radiation peut être demandée par l'emprunteur lui-même. Lorsque celle-ci n'est pas demandée par l'emprunteur, elle doit intervenir d'office et dans tous les cas à l'issue d'un délai d'un an à compter de la date de fin du prêt précédent.

Les informations concernant chaque prêt sont conservées jusqu'à la fin du quatrième mois suivant la restitution de l'objet du prêt. Au-delà de ce délai, les informations sur support magnétique sont détruites ; elles ne peuvent être conservées sur support papier que pour les besoins et la durée d'un contentieux éventuel.

S'agissant des documents d'archives, les informations relatives aux consultations sont conservées jusqu'au prochain récolement — inventaire — et dans la limite d'une durée maximum de dix ans.

Article 5
Destinataires des informations

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des informations :
— les services chargés de la gestion des prêts ou des consultations de documents d'archives ;
— leurs agents habilités pour les tâches comptables administratives ou des contentieux ;
— les supérieurs hiérarchiques de ces personnels et les membres des services d'inspection ;

Article 6
Enregistrement et traitements complémentaires

Les traitements dont les finalités sont celles définies à l'article 2 ci-dessus mais qui comportent l'enregistrement d'informations n'appartenant pas aux catégories énumérées à l'article 3 ou aboutissant à la transmission d'infor-

mations à des destinataires autres que ceux définis à l'article 5 doivent faire l'objet de demandes d'avis complémentaires.

Article 7

La norme simplifiée instituée par la délibération n° 80-17 du 6 mai 1980 est abrogée.

Délibération n° 99-028 du 22 avril 1999 portant avis conforme sur un projet de décret présenté par le ministère de l'Emploi et de la Solidarité autorisant la Caisse mutuelle d'assurance maladie des cultes (CAMAC) et la Caisse mutuelle d'assurance vieillesse des cultes (CAMAVIC) à enregistrer des informations faisant apparaître directement ou indirectement l'appartenance religieuse de leurs assurés

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 notamment l'article 31, ensemble le décret n° 78-774 du 17 juillet 1978,

Vu le code de la sécurité sociale, notamment les articles L.381-12 et L.721-4 et suivants ;

Vu la délibération n° 98-071 du 7 juillet 1998 portant avis conforme sur un projet de décret présenté par le ministère de l'emploi et de la solidarité autorisant la caisse mutuelle d'assurance maladie des cultes (Camac) et la caisse mutuelle d'assurance vieillesse des cultes (Camavic) à enregistrer des informations faisant apparaître directement ou indirectement l'appartenance religieuse de leurs assurés ;

Vu l'avis de la section sociale du Conseil d'Etat en date du 9 octobre 1998 ;

Vu le nouveau projet de décret présenté par le ministère de l'emploi et de la solidarité ;

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

Considérant que conformément à l'article 31, alinéa 3, de la loi du 6 janvier 1978 le ministère de l'emploi et de la solidarité a saisi la CNIL, pour avis conforme, d'un projet de décret en Conseil d'Etat afin d'autoriser la CAMAC (caisse mutuelle d'assurance maladie des cultes) et la CAMAVIC (caisse mutuelle d'assurance vieillesse des cultes) à traiter des informations nominatives faisant apparaître directement ou indirectement les opinions religieuses de leurs assurés ;

Considérant que la Commission s'est déjà prononcée par délibération n° 98-071 du 7 juillet 1998 sur un tel projet de décret ; que la section sociale du Conseil d'Etat, dans sa séance du 6 octobre 1998, a procédé à des modifications du texte précédemment soumis à la CNIL ;

Considérant que ces modifications portent sur la suppression de la mention « compte tenu des particularités de gestion qui en découlent au regard des spécificités de la vie religieuse et de la diversité des cultes » ; que la suppression de cette mention n'entraîne pas de modification substantielle au projet de décret dès lors qu'il s'agit de ne faire référence qu'à la seule base légale ayant institué le régime des cultes ;

Considérant, en conséquence, que cette modification n'appelle pas d'observations de la Commission ;

Emet un **avis conforme** au projet de décret en Conseil d'Etat présenté par le ministère de l'emploi et de la solidarité.

Délibération n° 99-029 du 4 mai 1999 portant avis sur un modèle-type de traitement présenté par le ministère de la Justice concernant le suivi des affaires pénales du Parquet général des cours d'appel

(Demande d'avis nº 532651)

La Commission nationale de l'informatique et des libertés,

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

Vu les articles 34 à 38 du code de procédure pénale ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, pris ensemble le décret nº 78-774 du 17 juillet 1978 ;

Vu le décret nº 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 le projet d'arrêté présenté par le Garde des Sceaux, Ministre de la Justice ;

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

Considérant que le ministère de la Justice a saisi la Commission d'une demande d'avis relative à la création d'un modèle-type appelé à être mis en œuvre dans les Parquets généraux près les cours d'appel ;

Considérant que le traitement a pour finalité de permettre le suivi des procédures relevant de la compétence du Parquet général, le contrôle des délais ainsi que la production de statistiques ;

Considérant que le projet d'arrêté prévoit que, s'agissant des personnes mises en cause, sont enregistrés les nom, nom d'alias (le cas échéant), prénoms, date de naissance, sexe, nationalité, profession, adresse ou lieu de détention, infractions reprochées (résumé des faits, date et qualification juridique), décisions prises dans la procédure en cours ;

Considérant qu'il y a lieu de préciser la notion de « personnes mises en cause » qui doit exclusivement viser les témoins assistés, les personnes mises en examen, les prévenus et les accusés ainsi que les personnes mises en cause dans une enquête préliminaire ou de flagrance lorsqu'il en est rendu compte par le Procureur de la République au Parquet général ;

Considérant que, s'agissant des parties civiles, des personnes civilement responsables, des représentants légaux ou des autres personnes en cause (plaignants, victimes, témoins), sont enregistrés les nom (raison sociale pour les personnes morales), prénoms, sexe, adresse ou domicile élu et qualité ; que, s'agissant des avoués, avocats, huissiers, notaires, experts judiciaires, mandataires de justice, magistrats consulaires, sont enregistrés les nom, prénoms, et numéro de téléphone professionnel ; que, s'agissant du magistrat chargé du dossier, sont enregistrés les fonctions, nom et prénoms ;

Considérant que ces informations sont pertinentes au regard de la finalité du traitement ;

Considérant que le traitement permettra d'enregistrer un résumé de chaque affaire dans une zone de texte libre ; qu'il convient à cet égard de rappeler que les informations enregistrées doivent être adéquates, pertinentes et non excessives au regard de la finalité du traitement ; qu'elles doivent en outre être objectives et ne sauraient par conséquent résulter d'un jugement de valeur ou d'une appréciation du comportement des personnes ; que les personnes concernées par le traitement disposent, conformément aux dispositions de l'article 34 de la loi du 6 janvier 1978, d'un droit d'accès à ces informations ;

Considérant que le projet d'arrêté prévoit que les informations seront conservées pendant la durée de prescription de la peine, soit 20 ans pour les crimes, 5 ans pour les délits et 2 ans pour les contraventions ; qu'une telle durée de conservation paraît excessive au regard des finalités assignées au traitement ; qu'il y a lieu, en ce qui concerne les crimes, de ramener cette durée à 5 ans à compter du jour où la dernière décision est devenue définitive ;

Considérant que le traitement sera mis en œuvre au sein du Parquet général de chaque Cour d'appel et ne sera accessible qu'aux magistrats et fonctionnaires habilités de ce parquet ; que le directeur des affaires criminelles et des grâces du ministère de la Justice et les magistrats ou fonctionnaires habilités de la direction des affaires criminelles et des grâces pourront être rendus destinataires d'informations nominatives issues de ce traitement ;

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 des greffiers en chef des cours d'appel ; que l'information relative à ce droit d'accès sera effectuée par l'apposition d'une affiche dans les services administratifs du parquet ;

Considérant qu'aux termes de l'article 37 de la loi du 6 janvier 1978, un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information qui y figure ; que l'article 7 du projet d'arrêté indique que les informations seront mises à jour en cas d'amnistie ou de réhabilitation ;

Considérant que le projet d'arrêté prévoit que les chefs de cours d'appel qui souhaiteront mettre en œuvre un tel traitement adresseront à la Commission nationale de l'informatique et des libertés une déclaration de conformité au présent modèle-type, accompagnée d'une annexe précisant les mesures prises pour assurer la sécurité et la confidentialité des informations traitées ;

Emet un avis favorable sous les réserves suivantes :

— à l'article 3 du projet d'arrêté, les mots « personnes mises en cause » doivent être remplacés par les mots « les témoins assistés, les personnes mises en examen, les prévenus, les accusés ainsi que les personnes mises en cause dans une enquête préliminaire ou de flagrance lorsqu'il en est rendu compte par le Procureur de la République au Parquet général » ;
— l'article 7 est ainsi rédigé :
« Les informations nominatives sont conservées pendant une durée de 5 ans à compter du jour où la dernière décision est devenue définitive, avec mise à jour en cas d'amnistie ou de réhabilitation. Lorsque, dans ce délai, un recours est formé devant la Cour Européenne des Droits de l'Homme, les informations sont conservées jusqu'à la date de la décision définitive de la Cour. »

Délibération n° 99-032 du 27 mai 1999 portant avis sur la mise en œuvre d'un traitement automatisé d'informations nominatives présenté par le Comité opérationnel de lutte contre le travail illégal de Paris concernant la coordination de la lutte contre le travail illégal

(Demande d'avis n° 648710)

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° 97-210 du 11 mars 1997 relative au renforcement de la lutte contre le travail illégal ;

Vu l'article 777-3 du code de procédure pénale ;

Vu les articles L 324-9 et suivants 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 n° 97-213 du 11 mars 1997 relatif à la coordination de la lutte contre le travail illégal ;

Vu le projet de décision portant création d'un fichier informatisé placé sous l'autorité du procureur de la République près le Tribunal de Grande Instance de Paris en sa qualité de président du Comité Opérationnel de Lutte contre le Travail Illégal de Paris ayant pour finalité la gestion et la centralisation des procès verbaux relatifs aux infractions de travail illégal ;

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 procureur de la République près le Tribunal de Grande Instance de Paris en sa qualité de président du Comité Opérationnel de Lutte

contre le Travail Illégal (COLTI) de Paris a saisi la Commission d'une demande d'avis concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion et la centralisation des procès verbaux relatifs aux infractions de travail illégal ;

Considérant que la loi du 31 décembre 1991 relative à la lutte contre le travail clandestin a introduit par les articles L 324-9 et suivants du code du travail un certain nombre de dispositions destinées à lutter contre le travail illégal : que la multitude des corps de contrôle concernés par la lutte contre le travail illégal et la multiplicité des missions qui leurs sont imparties rend nécessaire leur coordination ;

Considérant que le décret du 11 mars 1997 prévoit la coordination de la lutte contre le travail illégal et étend les pouvoirs des agents de contrôle en développant les possibilités d'échanges d'information entre les services de contrôle afin d'accroître l'efficacité des enquêtes.

Considérant que le COLTI a pour mission de coordonner les opérations de contrôle, de recenser les moyens nécessaires à ces opérations, de mettre à la disposition des URSSAF et des services des impôts les informations nécessaires au recouvrement des cotisations sociales et des impôts et de veiller aux échanges d'informations en direction des services de protection sociale en application de l'article L 324-13 du code du travail et d'établir des statistiques destinées à mieux appréhender le phénomène du travail illégal ;

Considérant que le COLTI de Paris a mis en œuvre un traitement automatisé d'informations nominatives destiné à faciliter l'accomplissement de ces missions et à favoriser la coordination des services ;

Considérant que les informations issues des procès-verbaux dressés par les corps de contrôle sont enregistrées dans le traitement automatisé par le secrétaire permanent du COLTI ;

Considérant que les informations enregistrées sont la raison sociale de l'entreprise, la forme juridique, le numéro de RCS ou de SIRET, la nationalité de l'entreprise si elle est étrangère, l'adresse du siège social et des établissements secondaires, le secteur d'activité, le lieu des faits, le nombre de salariés, le nom, prénom, date de naissance, nationalité, sexe du ou des mis en cause, la qualification du dirigeant au sein de l'entreprise, la qualification du salarié mis en cause pour sa responsabilité pénale personnelle, l'identité du donneur d'ordre en cas de recours au travail dissimulé, les infractions constatées et reprochées à chaque mis en cause, les suites judiciaires du procès verbal (classement, poursuite par citation directe, convocation par officier de police judiciaire, ouverture d'information), les condamnations judiciaires prononcées en première instance et appel, les suites fiscales, sociales ou sur les aides de l'Etat, s'agissant des salariés le nombre, la nationalité, le sexe, le type d'emploi exercé illégalement et les infractions reprochées à l'employeur ;

Considérant qu'au regard de l'article 30 de la loi du 6 janvier 1978 le COLTI, placé sous la direction du procureur de la République, est habilité à traiter de façon informatisée le suivi des infractions ;

Considérant que ces informations qui ne sont nominatives que pour les dirigeants des entreprises en cause paraissent adéquates et non excessives au regard de la finalité poursuivie ; que les informations relatives aux salariés victimes ne sont que des dénombrements dépourvus de tout caractère directement ou indirectement nominatif ;

Considérant que l'accès aux informations est ouvert aux corps de contrôles visés à l'article L 324-12 du code du travail et que la consultation porte sur l'ensemble des données contenues dans le fichier ; que toutefois, seule la personne représentant l'administration concernée au sein du COLTI disposera d'un accès direct aux informations contenues dans le traitement ;

Considérant que ces informations seront conservées pendant une durée de 5 ans ; que cette durée est justifiée par l'article L 324-13-2 du code du travail qui autorise l'administration à refuser d'accorder des aides publiques à l'emploi ou à la formation professionnelle pendant une durée de 5 ans aux personnes physiques et morales ayant fait l'objet d'un procès verbal pour travail dissimulé ou pour marchandage ;

Considérant que la mise à jour des informations sera assurée par le secrétariat permanent du COLTI en temps réel en fonction des poursuites exercées par le Parquet de Paris et des décisions rendues par le Tribunal correctionnel et par la Cour d'appel ; qu'en cas de non-lieu ou de relaxe les informations nominatives relatives aux dirigeants devront être effacées dans un délai de 10 jours à compter de la date où la décision est devenue définitive ;

Considérant que l'information des personnes concernées sera faite lors de l'établissement des procédures dressées par les agents de contrôle et que l'acte réglementaire sera affiché dans les locaux de chacun des services habilités à constater les infractions de travail dissimulé ;

Emet un **avis favorable** au projet de décision présenté par le Procureur de la République près le Tribunal de grande Instance de Paris sous réserve que l'acte réglementaire soit complété ainsi qu'il suit « En cas de relaxe ou de non lieu, les informations nominatives relatives aux dirigeants sont effacées dans un délai de dix jours à compter de la date où la décision est devenue définitive. »

Délibération n° 99-036 du 8 juillet 1999 portant avis sur un projet de modification de l'arrêté du 23 décembre 1997 portant creation 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 ou les forces d'occupation

(Demande d'avis nº 553059)

La Commission nationale de l'informatique et des libertés,

Vu la Convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 31 ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu le décret nº 78-774 du 17 juillet 1978, pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le décret nº 97-1174 du 23 décembre 1997 pris en application de l'article 31 alinéa 3 de la loi du 6 janvier 1978 ;

Vu l'arrêté du 25 mars 1997 portant création de la mission d'étude sur la spoliation durant l'occupation des biens appartenant aux juifs résidant en France ;

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 ;

Vu le projet d'arrêté présenté par le Secrétaire Général du Gouvernement ;

Vu la délibération de la CNIL nº 97 092 du 2 décembre 1997 relative a 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 mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy ;

Vu la délibération de la CNIL nº 97 093 du 2 décembre 1997 portant avis sur un projet d'arrêté du premier ministre relatif au traitement mis en œuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy ;

Après avoir entendu Monsieur Didier GASSE, Commissaire, en son rapport, et Madame Charlotte-Marie PITRAT, Commissaire du gouvernement en ses observations ;

Considérant que la Commission est saisie par le Secrétariat général du gouvernement, d'une demande d'avis modificative de 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 ;

Considérant que la modification a pour objet de compléter la liste des destinataires des informations nominatives afin d'y inclure les personnes mandatées par le président de la mission appartenant aux organismes suivants :
— la Poste,
— les établissements de crédit et les entreprises d'investissement,
— les sociétés d'assurance, mutuelles d'assurance, agents généraux d'assurance, courtiers en assurance et sociétés de courtage en assurance,
— les offices notariaux,
— les sociétés de perception et de répartition des droits d'auteur et des droits des artistes-interprètes mentionnées à l'article L.321-1 du code de la propriété intellectuelle,
en tant que les informations sont nécessaires à l'accomplissement de la tâche qui leur a été confiée.

Considérant qu'il résulte du projet de modification que les destinataires n'auront connaissance de ces informations que dans la mesure où cela est nécessaire à l'accomplissement des tâches qui leur sont confiées ; qu'en outre chaque destinataire sera nominativement mandaté par la président de la mission ; qu'enfin chaque destinataire, avant d'être mandaté par le président de la mission s'engagera par écrit à respecter la confidentialité des données nominatives recueillies dans le cadre des travaux effectués pour le compte de la mission ;

Considérant que la mission tient à jour la liste des personnes mandatées par son président ;

Emet un **avis favorable** sur le projet d'arrêté modificatif présenté par le Secrétariat général du gouvernement.

Délibération n° 99-037 du 8 juillet 1999 portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête « handicaps — incapacités — dépendances » menée auprès des ménages

(Demande d'avis n° 644306)

La Commission nationale de l'informatique et des libertés ;

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 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 13 juillet 1998 portant création d'un traitement automatisé d'informations nominatives relatif à l'enquête « Vie Quotidienne et Santé » ;

Après avoir entendu Monsieur Guy Rosier, Commissaire, 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 l'INSEE, d'une demande d'avis concernant la mise en œuvre d'une enquête « Handicaps — Incapacités-Dépendances » menée auprès des ménages, dite « HID-ménages » ;

Considérant que l'objectif poursuivi par l'enquête est de disposer de données nationales sur l'incapacité et la dépendance, l'origine et les causes des problèmes rencontrés par les personnes, ainsi que sur les conséquences en résultant pour leur insertion dans la société ; qu'elle a enfin pour but d'évaluer le niveau et la nature des aides qui pourraient être affectées à la population concernée ;

Considérant que cette enquête sera menée auprès de 20 000 personnes ; que ces personnes seront tirées au sort dans la base de sondage constituée lors de l'enquête « Vie Quotidienne et Santé », enquête facultative, associée au recensement général de la population de 1999 ; que cette enquête dite « de filtrage » a permis de détecter les personnes en situation de « handicap-incapacité-dépendance » ;

Considérant que l'enquête HID auprès des ménages donnera lieu à deux interrogations des personnes, à deux ans d'intervalle ; que la première phase de collecte des données aura lieu fin 1999 ;

Considérant que l'enquête n'a aucun caractère obligatoire ;

Considérant que le recueil des données se fera directement auprès de la personne concernée ; que celle-ci pourra autoriser l'un de ses proches à répondre, si elle le souhaite ;

Considérant que les catégories de données enregistrées concerneront l'identité, les causes et origines des incapacités, la description des incapacités, l'environnement socio-familial, les conditions de logement et l'environne-

ment du logement, la scolarité et les diplômes, l'emploi, la formation et la profession, les types et les montants de revenus en tranches, la situation juridique et administrative de la personne interrogée ;

Considérant que ces données sont pertinentes, adéquates et non excessives au regard de la finalité du traitement ;

Considérant qu'à l'issue de l'entretien, l'enquêteur demandera les coordonnées d'un proche susceptible d'indiquer où contacter la personne concernée par l'enquête pour la seconde interrogation ; qu'il convient de prendre acte de l'engagement de l'institut national de la statistique et des études économiques d'informer cette personne relais de ce que ses coordonnées ont été communiquées à l'INSEE afin qu'elle puisse s'y opposer ;

Considérant que les agents spécialement habilités au sein de l'INSEE seront les seuls destinataires des données recueillies ; que la direction de la recherche, des études, de l'évaluation et des statistiques du ministère de l'emploi et de la solidarité, obtiendra, conformément aux dispositions de l'article 7Bis de la loi du 7 juin 1951, un fichier d'enquête anonyme comportant les codes commune, moyennant la signature d'une convention avec l'INSEE et un avis favorable de la CNIL ;

Considérant que le droit d'accès, tel que prévu par l'article 34 de la loi du 6 janvier 1978, s'exercera auprès des directions régionales de l'INSEE concernées ;

Dans ces conditions, **émet** un **avis favorable** au projet d'arrêté portant création du traitement envisagé. Sous réserve que son article 3 soit complété de la manière suivante : « Les agents spécialement habilités au sein de l'INSEE sont les seuls destinataires des données recueillies ».

Délibération n° 99-038 du 8 juillet 1999 portant avis sur le projet d'acte réglementaire modificatif présenté par la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) concernant le traitement automatisé d'informations nominatives « ANAISS » (Application nationale informatique des services sociaux)

La Commission nationale de l'informatique et des libertés,

Vu la Directive n° 95/46 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 relative à l'Informatique, aux fichiers et aux libertés, ensemble le décret d'application n° 78-774 du 17 juillet 1978 ;

Vu la délibération n° 94-063 du 28 juin 1994 relative à la demande d'avis de la Commission Nationale d'Assurance Maladie des Travailleurs Salariés relative à la mise en œuvre d'un traitement automatisé d'informations nominatives dénommé « ANAISS » de gestion des dossiers des assistants sociaux ;

Vu le projet d'acte réglementaire modificatif présenté par la CNAMTS ;

Après avoir entendu Monsieur Maurice VIENNOIS, en son rapport et Madame Charlotte-Marie PITRAT, Commissaire du gouvernement, en ses observations ;

Considérant que la CNAMTS a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis modificative du traitement ANAISS ayant pour objet de compléter la gestion informatisée des dossiers des assistants sociaux par deux fonctionnalités complémentaires ;

Considérant qu'aux termes de la demande d'avis modificative présentée, il s'agit :
— d'une part, d'ouvrir la possibilité aux assistants sociaux des unités locales des services sociaux d'interroger, selon différents critères, la base des dossiers sociaux informatisés afin de pouvoir mener des actions, soit personnalisées, soit collectives de travail social, plus adaptées en faveur des populations suivies,
— d'autre part, de permettre la transmission aux échelons régionaux et nationaux du service social, d'informations individuelles sur les difficultés sociales rencontrées par les personnes aidées et les actions entreprises afin d'élaborer des politiques d'actions sociales appropriées ;

Considérant que l'organisation d'actions collectives adaptées en faveur des personnes aidées nécessite de disposer d'informations sur les difficultés rencontrées par ces personnes et en conséquence d'utiliser certaines des données contenues dans les dossiers sociaux informatisés ;

Considérant que cette finalité est légitime ;

Considérant qu'il est en particulier envisagé de recourir à des codifications qui détaillent les difficultés rencontrées par les personnes suivies et sont d'ores et déjà utilisées dans le cadre de la gestion individuelle de leurs dossiers ;

Considérant que, ainsi que la Commission l'a rappelé dans l'avis rendu le 28 juin 1994, il appartient à l'assistant social ayant en charge la personne ou la famille, d'apprécier, eu égard aux difficultés sociales desdites personnes, la nature des informations à faire figurer dans le dossier ; qu'il lui revient ainsi de déterminer les caractéristiques de la situation de ces personnes et le type d'action à mentionner dans le dossier informatisé ;

Considérant toutefois que eu égard aux particularités des situations sociales rencontrées il peut s'avérer qu'aucun des codes proposés ne corresponde à la situation constatée ou que ce code la décrive de manière inadéquate ;

Considérant ainsi que la saisie de ces informations ne peut présenter un caractère systématique ;

Considérant en outre que certaines codifications, par leurs intitulés, relèvent d'une appréciation subjective de l'assistant social ; que, dès lors, leur exploitation à des fins d'organisation d'actions collectives de travail social demande à être évaluée au terme d'une année de mise en œuvre effective de telle sorte, en particulier, que les codifications retenues puissent le cas échéant, être améliorées ainsi que la CNAMTS s'y est d'ailleurs engagée ;

Considérant que la CNAMTS souhaite également que les informations enregistrées dans les dossiers sociaux individuels soient transmises aux échelons régionaux et nationaux du service social en vue d'exploitations statistiques

destinées à faire ressortir les principales caractéristiques et problèmes des bénéficiaires ainsi que les résultats des interventions sociales ;

Considérant que, pour éviter l'identification des personnes, ont été supprimées, à la demande de la Commission, les données relatives à l'état civil des bénéficiaires et des assurés, aux numéros les identifiant dans les différents organismes sociaux concernés, à l'identification des personnels sociaux ;

Considérant que la CNAMTS s'est par ailleurs engagée à ne produire aucune statistique correspondant à des groupes de moins de dix personnes et, de façon générale, à prendre toutes mesures nécessaires pour éviter, par recoupement d'informations, l'identification des personnes ;

Considérant que les mesures ainsi prises pour garantir la confidentialité de ces informations sont satisfaisantes ;

Considérant toutefois qu'il avait été envisagé de transmettre, sous forme détaillée, les codifications relatives aux difficultés rencontrées par les personnes aidées ;

Considérant que, eu égard à la finalité statistique des traitements envisagés, la transmission sous cette forme de ces informations n'est pas pertinente et adéquate ; qu'en conséquence la CNAMTS a proposé que les intitulés des codifications soient regroupés en catégories plus objectives ;

Considérant qu'il convient de prendre acte des modifications ainsi apportées tout en demandant à disposer d'un bilan des traitements statistiques effectués au terme d'un délai d'un an de mise en œuvre ;

Considérant que les seuls utilisateurs du traitement sont, au plan local, les assistants sociaux de l'unité du service social, y compris l'assistant social responsable de l'unité, les personnels administratifs assurant le secrétariat du service placés sous la responsabilité des assistants sociaux ; qu'en cas de réalisation d'actions collectives, les assistants sociaux concernés pourront être habilités, dans l'intérêt des personnes, à avoir accès à des informations concernant des assurés dont ils n'assurent pas habituellement le suivi ;

Considérant que les procédures d'habilitation doivent être définies en concertation avec les assistants sociaux et doivent être conçues pour assurer un accès différencié aux informations, sous forme de codes d'identification et d'accès personnalisés ;

Considérant que dans les échelons régionaux et nationaux du service social, seuls les personnels habilités de ce service pourront avoir accès aux bases statistiques ;

Considérant que les informations appelées à être communiquées aux échelons régionaux et nationaux seront télétransmises ;

Considérant à cet égard, que pour éviter tout accès incontrôlé à la base, il importe que les opérations de télétransmission soient réalisées à l'initiative des services locaux ;

Considérant en outre qu'il convient de recommander la mise en place soit d'une télémaintenance sur base fictive, soit d'une maintenance sur site ;

Considérant qu'un dispositif de journalisation des interrogations doit être mis en place tant au plan local qu'aux niveaux régionaux et nationaux ;

Prenant acte qu'aux termes de l'acte réglementaire présenté, les informations sont enregistrées dans le traitement ANAISS en accord avec le bénéficiaire de l'aide ;

Considérant que tout assuré social demandeur d'une aide peut s'opposer à ce que des informations le concernant fassent l'objet d'un traitement automatisé d'informations nominatives ;

Considérant en conséquence qu'il doit être clairement informé de l'existence de son droit d'opposition, des conséquences éventuelles d'un refus à l'égard du traitement de sa demande, ainsi que des modalités d'exercice de son droit d'accès et de rectification à l'ensemble des renseignements mémorisés le concernant ; que la Commission devra avoir connaissance des dispositions pratiques prises à cet effet ;

Emet un **avis favorable** à la mise en œuvre, pour une durée expérimentale d'un an, des nouvelles finalités du traitement ANAISS,

Demande à être saisie au terme de ce délai d'un bilan évaluant, tant pour la réalisation des actions collectives que pour les transmissions d'informations à des fins statistiques, la pertinence des informations utilisées et en particulier de celles relatives aux difficultés rencontrées ;

Souhaite avoir connaissance des dispositions retenues en pratique pour informer les assurés des droits qui leur sont reconnus au titre de la loi du 6 janvier 1978.

Délibération n° 99-041 du 8 juillet 1999 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 traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et 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 le projet de formulaire de déclaration des traitements de données personnelles mis en œuvre dans le cadre d'un site Internet annexé à la présente délibération ;

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, 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 deux périodes d'expérimentation, la présentation de ce formulaire a été formellement modifiée ; qu'il convient de recueillir les observations des déclarants et tout particulièrement des associations professionnelles concernées sur la nouvelle présentation du formulaire ;

Décide d'adopter pour une période de six mois le modèle de formulaire de déclaration annexé à la présente délibération.

Délibération n° 99-045 du 5 octobre 1999 portant avis sur un projet d'arrêté du ministre de l'Economie, des Finances et de l'Industrie concernant un traitement mis en œuvre par le service TRACFIN

(Demande d'avis n° 503656)

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 relative à l'informatique, aux fichiers et aux libertés, ainsi que son décret d'application n° 78-774 du 17 juillet 1978 ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi n° 90-614 du 12 juillet 1990 relative à la participation des organismes financiers à la lutte contre le blanchiment des capitaux provenant du trafic de stupéfiants, modifiée par la loi n° 93-122 du 29 janvier 1993, la loi n° 96-392 du 13 mai 1996, la loi n° 98-546 du 2 juillet 1998, et notamment ses articles 16 et 22 ;

Vu le décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du renseignement et de l'action contre les circuits financiers clandestins (TRACFIN) ;

Vu le décret n° 91-160 du 13 février 1991 fixant les conditions d'application de la loi n° 90-614 du 12 juillet 1990 ;

Vu le projet d'arrêté présenté par le ministère de l'économie, des finances et de l'industrie ;

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, des finances et de l'industrie a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis relative à un traitement, dénommé « TRACINFO », qui est mis en œuvre par la cellule Tracfin, dont l'une des missions est de recevoir et d'analyser les déclarations, dites de soupçon, adressées par les institutions

financières et les personnes qui réalisent, contrôlent ou conseillent des opérations portant sur l'acquisition, la vente, la cession ou la location de biens immobiliers, lorsqu'elles détectent des opérations financières inhabituelles ou suspectes qui paraissent liées au blanchiment des capitaux provenant du trafic de stupéfiants ou de l'activité d'organisations criminelles, dans le but d'en aviser le procureur de la République ;

Considérant que la finalité du traitement « TRACINFO » est d'apporter une aide à la lutte contre les circuits financiers clandestins et le blanchiment de l'argent à partir des renseignements portés sur les déclarations de soupçon, et plus particulièrement :
— l'enregistrement, la consultation des déclarations et la réalisation des analyses nécessaires pour appréhender les opérations financières complexes qui donnent lieu à plusieurs déclarations,
— l'édition des accusés de réception prévus à l'article 6 de la loi du 12 juillet 1990,
— le suivi des suites données aux enquêtes réalisées,
— la tenue du fichier des personnes physiques ou morales soupçonnées de participer à des circuits financiers clandestins liés au trafic de stupéfiants ou à l'activité d'organisations criminelles sur la base d'une déclaration,
— la gestion des informations relatives à l'identité des dirigeants des organismes financiers et de leurs préposés qui sont en charge des relations avec la cellule Tracfin ;

Considérant que les informations ainsi enregistrées dans l'application ne peuvent, en aucun cas, être utilisées à des fins étrangères à l'application de la loi du 12 juillet 1990 ;

Considérant que les catégories d'informations traitées seront nécessairement en rapport direct avec une déclaration de soupçon et concernent :
— pour les personnes physiques impliquées ou soupçonnées : le nom, le prénom, le surnom, le sexe, la nationalité, la date et le lieu de naissance, le nom des ascendants, la situation familiale, les adresses, le n° de téléphone, la profession, l'employeur, les références de la pièce d'identité,
— pour les personnes morales : la raison sociale, la forme juridique, la nationalité, l'adresse, le n° de téléphone, l'identité des dirigeants et des principaux actionnaires,
— pour les déclarations de soupçon : le type de déclaration, l'organisme financier déclarant, le n° de compte, le nom de l'enquêteur, la description de l'affaire, l'origine et la description des mouvements financiers, les suites apportées,
— pour les organismes financiers : l'identité, l'habilitation et le n° de téléphone des correspondants, les déclarations de soupçon effectuées ;

Considérant que ne sont pas conservés dans le traitement l'ensemble des opérations opérées sur les comptes ayant fait l'objet d'une déclaration de soupçon, mais les seuls mouvements financiers suspects portés sur la déclaration ; que l'identité des ascendants n'est saisie que dans les cas d'affaires de blanchiment de trafic de type familial ou pour assurer une meilleure identification des personnes ;

Considérant, en outre, que les zones « commentaires » prévues dans l'application ne devront comporter que des informations indispensables pour le traitement de l'affaire dans laquelle la personne est soupçonnée ou impliquée ; que le projet d'acte réglementaire devra être complété sur ce point ;

Considérant que le délai maximum de conservation des déclarations de soupçon et des renseignements obtenus par voie d'enquête est de dix années à compter de leur réception ; que cette durée ne peut en aucun cas être prorogée ; que toutefois, cette règle ne s'oppose pas à l'effacement immédiat des informations concernant des affaires pour lesquelles la cellule Tracfin est en possession d'éléments suffisants pour lever sans équivoque tout soupçon ;

Considérant que le traitement « TRACINFO » est purement interne à la cellule Tracfin ; que seuls des agents de la cellule Tracfin dûment habilités bénéficient d'un accès direct au traitement ;

Considérant que les informations traitées peuvent être communiquées :
— aux procureurs de la République,
— aux fonctionnaires de l'Office central de répression de la grande délinquance financières, en qualité d'officiers de police judiciaire désignés par le ministère de l'intérieur au titre de l'article 16 de la loi du 12 juillet 1990,
— aux services des douanes,
— aux autorités de contrôle des organismes financiers au sens de l'article 16 de la loi précitée,
— aux autorités étrangères exerçant des compétences analogues à la cellule Tracfin, sur la base d'accords administratifs d'assistance concernant l'échange de renseignements ;

Considérant que si ces personnes peuvent être rendues destinataires des analyses et expertises préparées par la cellule Tracfin à partir de données issues du traitement « TRACINFO », celles-ci ne peuvent pas avoir communication d'informations directement issues d'une déclaration de soupçon, et notamment de précisions sur la déclaration à l'origine d'une procédure ou sur son auteur ; que l'article 4 du projet d'arrêté devra être complété en ce sens ;

Considérant, s'agissant des flux transfrontières de données, que l'article 22 de la loi du 12 juillet 1990 prévoit que ceux-ci doivent respecter les dispositions législatives et les conventions internationales applicables en matière de protection de la vie privée et de communication des données à caractère nominatif ;

Considérant cependant que, dès lors que l'efficacité de la lutte contre les trafics de stupéfiants et des réseaux de blanchiment rend indispensables l'échange international de renseignements nominatifs, la mise en place d'une coopération entre la cellule Tracfin et ses partenaires étrangers ne peut pas raisonnablement être subordonnée à l'existence d'accords par lesquels ceux-ci prendraient l'engagement préalable d'appliquer les règles susrappelées ; qu'au surplus, la réflexion progresse, au sein des instances internationales compétentes en matière de blanchiment de capitaux, pour promouvoir des standards communs d'échanges d'information dans le respect des principes relatifs au respect de la vie privée et à la protection des données ; que l'engagement a été pris, à cette fin, d'accompagner chaque échange d'informations avec un homologue étranger d'une mention expresse rappelant la nécessité de respecter les conditions de confidentialité et de finalité et de prendre les mesures appropriées permettant d'assurer un contrôle des dispositions relatives au respect de la vie privée ; que les responsables de la cellule Tracfin s'engagent également à rappeler, lors des négociations des accords de coopération, l'attachement aux principes de la protection des données et à y sensibiliser leurs partenaires ;

Considérant que le traitement « TRACINFO » et les « dossiers-papier » auxquels il renvoie, intéressant la sécurité publique, le droit d'accès les concer-

nant doit s'exercer auprès de la Commission nationale de l'informatique et des libertés conformément à l'article 39 de la loi du 6 janvier 1978 ; qu'en outre, afin de faciliter l'exercice du droit d'accès indirect en cas d'échange d'informations avec l'étranger, les membres de la CNIL chargés de l'exercice de ce droit d'accès indirect seront informés, au cas par cas et lorsque cela sera nécessaire, dans le strict respect des conditions de confidentialité requises, des références des autorités étrangères qui ont été destinataires d'informations nominatives ;

Considérant, que si l'application de la procédure de l'article 39 se justifie pour la plupart des informations enregistrées dans le traitement, rien ne s'oppose en revanche à l'application du droit d'accès direct de l'article 34 de la loi du 6 janvier 1978 pour les informations relatives aux correspondants Tracfin des organismes financiers ;

Emet un **avis favorable** sur le projet d'arrêté présenté par le ministère de l'économie, des finances et de l'industrie, compte tenu des engagements souscrits susanalysés et sous réserve que :
— l'article 2 soit complété au point c par le membre de phrase suivant : « les commentaires ne devant comporter que les informations objectives strictement indispensables pour le traitement de cette affaire »,
— l'article 4 soit complété d'un second alinéa, rédigé comme suit : « Toutefois, ces personnes et les autorités étrangères ne peuvent pas obtenir communication d'informations directement issues de déclarations de soupçon, et notamment de précisions sur la déclaration à l'origine d'une procédure ou sur son auteur. »
— l'article 6 soit rédigé comme suit : « Le droit d'accès aux informations figurant dans l'application TRACINFO s'exerce auprès de la Commission nationale de l'informatique et des libertés dans les conditions de l'article 39 de la loi du 6 janvier 1978, sauf en ce qui concerne les informations relatives aux correspondants Tracfin des organismes financiers qui exerceront leur droit d'accès et de rectification auprès de la cellule Tracfin conformément aux dispositions des articles 34 et suivants de la même loi. »

Délibération n° 99-050 du 28 octobre 1999 portant avis sur le projet d'arrêté, présenté par l'INSEE, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer les demandes de modification du NIR exprimées par les personnes nées en Algérie avant le 3 juillet 1962

(Demande d'avis n° 588076)

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 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 décret n° 82-103 du 22 janvier 1982 modifié relatif au répertoire national d'identification des personnes physiques ;

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 ;

Considérant que l'INSEE a saisi la Commission nationale de l'informatique et des libertés de la mise en œuvre d'un traitement automatisé d'informations nominatives destiné à gérer les demandes de modification du répertoire national d'identification des personnes physiques (RNIPP) exprimées par les personnes nées en Algérie avant le 3 juillet 1962 ;

Considérant que cette modification porte sur la modalité « lieu de naissance » du numéro d'inscription au répertoire (NIR) ; que cette modalité, actuellement exprimée par le code « 99 », est affectée à toutes les personnes nées hors du territoire français ; que la demande des personnes concernées vise à faire substituer au code « 99 » un code entre « 91 et 94 », significatif de leur commune ou lieu de naissance ;

Considérant que le traitement mis en œuvre par l'INSEE a pour objet de regrouper toutes les données nominatives sur les personnes nées en Algérie avant le 3 juillet 1962 qui lui seront transmises par les organismes d'assurance maladie, de les confronter au RNIPP, d'adresser une notification aux intéressés afin que ces derniers donnent leur consentement exprès à la modification de leur NIR, enfin de procéder à la modification souhaitée et la transmettre aux organismes de sécurité sociale habilités ;

Considérant que les données transmises à l'INSEE par les organismes de sécurité sociale sont les suivantes : nom, prénoms, date et lieu de naissance, sexe, adresse, NIR ;

Considérant que l'INSEE conserve les données pendant un délai de quatre mois au plus à compter de leur réception ;

Considérant que les seuls destinataires des informations traitées sont les agents habilités de l'INSEE ; que les agents habilités des organismes d'assurance maladie ont connaissance des NIR modifiés ;

Considérant que le droit d'accès organisé par l'article 34 de la loi du 6 janvier 1978, ainsi que le droit de rectification s'exercent auprès de la direction régionale de l'INSEE des Pays de la Loire ;

Emet un **avis favorable** au projet d'arrêté portant création du traitement.

Délibération n° 99-051 du 28 octobre 1999 portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 82-103 du 2 janvier 1982 relatif au répertoire national d'identification des personnes physiques

(Demande d'avis n° 588 076)

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 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 décret n° 82-103 du 22 janvier 1982 modifié relatif au répertoire national d'identification des personnes physiques ;

Vu le projet de décret en Conseil d'Etat relatif à la modification du RNIPP concernant les personnes nées en Algérie avant le 3 juillet 1962 ;

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

Considérant que la Commission est saisie d'un projet de décret en Conseil d'Etat modifiant le décret précité n° 82-103 du 22 janvier 1982, par l'ajout d'un article 4 bis qui permet, à toutes les personnes nées en Algérie avant le 3 juillet 1962, d'obtenir un nouveau numéro d'inscription au répertoire (NIR) ;

Considérant que le numéro d'inscription au répertoire des personnes nées en Algérie avant l'indépendance immatriculées postérieurement au 3 juillet 1962 ou n'ayant pu apporter la preuve d'une immatriculation antérieure, comporte le code « 99 », indicateur du lieu de naissance à l'étranger ;

Considérant que le projet de décret soumis à l'avis de la Commission prévoit de substituer au code « 99 », un code « lieu de naissance » fixé entre « 91 et 94 », pour tenir compte, en fonction de leur commune ou lieu de naissance, de l'indicatif des anciens départements d'Algérie ;

Considérant que cette procédure sera permanente pour les personnes demandant leur première inscription au répertoire national d'identification des personnes physiques ; que cette procédure aura un caractère exceptionnel pour les personnes déjà inscrites au répertoire ; que dans ce second cas, le décret subordonne la modification du NIR des personnes concernées à leur acceptation expresse dans un délai de deux mois de la proposition de modification qui leur est adressée par l'INSEE ;

Considérant que ces dispositions du projet de décret n'appellent pas d'observations particulières, dans la mesure où elles visent à satisfaire les demandes des personnes concernées ;

Emet un avis favorable au projet de décret qui lui est présenté.

Délibération n° 99-053 du 18 novembre 1999 portant avis sur le projet de règlement modifié du Comité de la réglementation bancaire relatif au fichier des incidents de remboursement des crédits aux particuliers (FICP)

La Commission nationale de l'informatique et des libertés,

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

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

Vu la loi n° 84-46 du 24 janvier 1984 sur l'activité et le contrôle des établissements de crédit ;

Vu la loi d'orientation n° 98-657 du 29 juillet 1998 relative à la lutte contre les exclusions ;

Vu le code de la Consommation, titre III du livre III ;

Vu le décret n° 78-774 du 17 juillet 1978, pris pour l'application des chapitres I à IV et VII de la loi du 6 janvier 1978 ;

Vu le règlement n° 90-05 du comité de la réglementation bancaire relatif au fonctionnement du fichier des incidents de remboursement des crédit aux particuliers (FICP) ;

Vu la délibération n° 89-108 du 26 septembre 1989 portant avis sur un projet de loi relatif à la prévention et au règlement judiciaire des difficultés liées au surendettement des ménages ;

Vu la délibération n° 90-29 du 6 mars 1990 portant avis sur le projet de règlement du comité de réglementation bancaire, relatif au FICP ;

Vu la délibération n° 93 019 du 2 mars 1993 portant avis sur le projet de règlement modifié du CRB relatif au FICP ;

Vu la délibération n° 96 019 du 19 mars 1996 portant avis sur le projet de règlement modifié du Comité de la réglementation bancaire relatif au fichier des incidents de remboursement des crédits aux particuliers (FICP) ;

Vu l'avis du comité consultatif institué par l'article 59 de la loi du 24 janvier 1984 dite loi bancaire, en date du 14 juin 1999 recommandant la modification de certaines dispositions du règlement n° 90-05 du Comité de la réglementation bancaire ;

Vu le projet de modification de ce règlement ;

Après avoir entendu Monsieur Pierre LECLERCQ en son rapport, et Madame Charlotte-Marie PITRAT, Commissaire du gouvernement, en ses observations ;

Considérant d'une part que la loi susvisée du 29 juillet 1998 a apporté plusieurs modifications à la procédure de traitement des situations de surendettement, qui sont entrées en vigueur le 2 février 1999 ; que lesdites modifications rendent nécessaire, sur divers points, une mise à jour du règlement n° 90-05 précité ;

Considérant que d'autre part le comité consultatif a émis le 14 juin 1999 un avis proposant des aménagements susceptibles d'améliorer la prévention du surendettement ;

Considérant que conformément à l'article L 333-4 alinéa 1 du code de la consommation, le débiteur surendetté doit désormais être inscrit dans le FICP dès que sa demande a été jugée recevable par la Commission de surendettement ou par le juge en cas de recours contre la décision de cette dernière ;

Considérant cependant que la loi n'a précisé ni la durée de conservation de l'inscription au titre de la décision de recevabilité, ni les motifs de sa suppression ;

Considérant que le comité consultatif estime raisonnable de fixer cette durée de conservation à 2 ans avec possibilité de prorogations par périodes d'un an ;

Considérant que la radiation interviendrait dès que le débiteur bénéficie d'une mesure de traitement du surendettement ou en cas de clôture du dossier de surendettement pour quelque motif que ce soit ;

Considérant que ces dispositions n'appellent pas d'observations dès lors que l'information préalable du débiteur serait clairement effectuée ;

Considérant que la durée de conservation maximale des informations relatives aux mesures de traitement du surendettement a été portée par la loi du 29 juillet 1998 de 5 à 8 ans et qu'il n'est pas proposé par le comité consultatif d'allonger corrélativement, dans un souci d'homogénéisation des délais de conservation de l'ensemble des informations figurant au fichier, la durée de conservation des incidents de paiement caractérisés, qui demeure ainsi fixée à cinq ans ;

Considérant que dans la mesure où la loi a fixé elle même des durées précises pour chaque inscription, il n'apparaît désormais plus envisageable de modifier comme cela avait été le cas en 1993 et en 1996, les durées de conservation des informations enregistrées dans le fichier national ;

Considérant que la loi du 29 juillet 1998 a instauré de nouvelles mesures propres au traitement de l'insolvabilité durable et en a défini la durée de conservation qu'il s'agisse de mesures de suspension de l'exigibilité des créances autres qu'alimentaires ou fiscales (article L 331-7-1 alinéa 1) ou des mesures d'effacement total ou partiel des dettes autres qu'alimentaires ou fiscales (article L 331-7-1, alinéa 3) ;

Considérant que la durée de conservation des mesures de suspension est égale à leur durée d'exécution, sans pouvoir excéder 3 ans, la Commission de surendettement devant réexaminer le dossier à l'issue de cette période, conformément à l'article L.331-7-1 ;

Considérant que le Comité consultatif prévoit, en l'absence de précisions données par la loi, qu'une nouvelle inscription du débiteur au titre de la recevabilité devrait avoir lieu afin d'éviter une sortie provisoire du débiteur du fichier, entre la radiation de l'inscription au titre de la suspension et l'enregistrement d'une nouvelle mesure après examen ;

Considérant que cette proposition n'appelle pas d'observations dès lors que l'information préalable du débiteur aura été clairement effectuée ;

Considérant qu'il résulte de la loi du 29 juillet 1998 que les mesures d'effacement des créances doivent être inscrites pour une durée de 8 ans et que le Comité consultatif propose qu'il soit précisé l'absence de possibilité de radiation anticipée dans la mesure où la loi prévoit qu'aucun nouvel effacement ne doit intervenir pendant cette période pour des dettes similaires à celles qui ont donné lieu à effacement ;

Emet, dans ces conditions**,** un avis favorable au projet de règlement modifié qui lui a été présenté.

Délibération n° 99-054 du 18 novembre 1999 portant avis favorable au traitement automatisé d'informations nominatives mis en œuvre par le ministère de l'Agriculture et de la Pêche, à l'occasion du recensement général de l'agriculture (RGA)

(Demande d'avis nº 662113)

La Commission nationale de l'informatique et des libertés,

Vu la Convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement CEE 571/88 du Conseil portant organisation d'enquêtes communautaires sur la structure des exploitations agricoles, modifié par le règlement CE 2467/96 du 17 décembre 1996 ;

Vu la loi nº 51-711 du 7 juin 1951 modifiée, sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 79-18 du 3 janvier 1979 sur les archives ;

Vu le décret nº 78-774 du 17 juillet 1978 pris pour l'application de la loi susvisée de 1978 ;

Vu le projet d'arrêté du ministre de l'agriculture et de la pêche 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 ;

Considérant que la CNIL est saisie, par le ministère de l'agriculture et de la pêche, de la mise en œuvre d'un traitement automatisé d'informations nominatives lors du recensement général de l'agriculture qui doit avoir lieu en 2000, en métropole et dans les départements et territoires d'Outre-Mer ;

Considérant que le traitement considéré est réalisé sous la responsabilité du service central des enquêtes et d'études statistiques (SCEES), du ministère de l'agriculture et de la pêche ;

Considérant que le traitement informatisé des données recueillies lors du RGA a pour finalité :
— l'élaboration de statistiques anonymes, sur tout ou partie du recensement agricole, relatives aux caractéristiques des exploitations agricoles, à leur activité et aux personnes qui les dirigent, vivent ou travaillent dans celles-ci,
— l'alimentation de la base de sondage nominative des exploitations agricoles utilisée pour la réalisation d'enquêtes statistiques ultérieures, exhaustives ou par échantillonnage.

Considérant que les données collectées à l'occasion de cette enquête obligatoire concernent, pour chaque unité de production : l'identification de l'unité, sa structure et son environnement économique, l'utilisation du sol, les cheptels, l'équipement en matériel agricole, la population familiale et salariée vivant ou y travaillant, la main-d'œuvre occasionnelle ; que les données relatives aux personnes physiques qui dirigent, vivent ou travaillent sur l'unité de production ont trait à l'état civil, la situation familiale, le niveau et la nature de la formation acquise et des activités professionnelles ;

Considérant qu'après la collecte des données précitées, la suite des opérations du traitement automatisé ne comporte pas les nom et prénoms des exploitants ;

Considérant que les informations recueillies sont pertinentes, adéquates et non excessives au regard de la finalité du traitement ;

Considérant que les destinataires des informations collectées sont les agents habilités des services de statistique agricole du ministère de l'agriculture et de la pêche ainsi que les agents habilités de l'INSEE ; que les questionnaires sont versés aux Archives de France un an après la réalisation du RGA ;

Considérant que toutes les mesures prises paraissent de nature à garantir la sécurité et la confidentialité des informations ;

Considérant que le droit d'accès prévu par l'article 34 de la loi nº 78-17 du 6 janvier 1978 peut être exercé auprès du service central des enquêtes et études statistiques du ministère de l'agriculture ;

Emet un **avis favorable** au projet d'arrêté portant création du traitement.

Délibération n° 99-055 du 18 novembre 1999 relative à la gestion et aux négociations des biens immobiliers

(Norme simplifiée nº 21)

La Commission nationale de l'informatique et des libertés,

Vu les articles 6, 17 et 21 (1°) de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés habilitant la Commission nationale de l'informatique et des libertés à édicter, en vertu de son pouvoir réglementaire, des normes simplifiées concernant certains traitements automatisés d'informations nominatives ;

Considérant que pour l'application de l'article 17 susvisé, il faut entendre par norme simplifiée l'ensemble des conditions que doivent remplir certaines catégories les plus courantes de traitements pour être regardées comme ne comportant pas de risques d'atteinte à la vie privée et aux libertés et comme pouvant dès lors faire l'objet d'une déclaration simplifiée ;

Considérant que certains traitements automatisés, portant sur la gestion et les négociations des biens immobiliers sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné ;

Décide :

Norme simplifiée relative à la gestion et aux négociations des biens immobiliers

Article 1er

Les dispositions de la présente décision concernent les traitements automatisés d'informations nominatives relatifs à la gestion et aux négociations des biens immobiliers mis en œuvre par toute personne publique ou privée.

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée, ces traitements doivent :

— ne porter que sur des données objectives aisément contrôlables par les intéressés grâce à l'exercice du droit individuel d'accès ;

— n'appliquer à ces données que des logiciels dont les résultats puissent être facilement contrôlés ;

— ne pas procéder à des cessions ou locations des contenus des fichiers de l'organisme ;

— ne pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des fonctions énoncées à l'article 2 ci-dessous ;

— comporter des dispositions propres à assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi ;

— satisfaire en outre aux conditions énoncées aux articles 2 à 6 ci-dessous.

Article 2
Finalité du traitement

Le traitement ne doit pas avoir d'autres fonctions que :

a) d'établir le quittancement des loyers : l'émission de titres de recettes des locations et la gestion des relances, le décompte des taxes et charges y affé-

rentes, la régularisation des charges, les pièces comptables nécessaires au recouvrement et à la gestion des comptes des locataires concernés ;
b) d'assurer la gestion des sociétés civiles immobilières, des sociétés ayant pour objet la construction, des coopératives et des syndicats de copropriété, des associations syndicales libres et des immeubles en jouissance à temps partagé : la comptabilité de ces organismes, la tenue des comptes des intéressés, la convocation aux assemblées générales, les lettres de relance, les appels de fonds ;
c) d'établir la gestion des mandats de gérance : la comptabilité du mandat de gérance, la tenue des comptes des propriétaires, la tenue des comptes des locataires**,** la déclaration des revenus fonciers ;
d) d'assurer les opérations de négociation immobilière ;

Article 3
Catégories d'informations traitées

Dès lors que les dispositions de l'article 27 de la loi nº 78-17 du 6 janvier 1978 ont été respectées lors du recueil des informations traitées, celles-ci doivent relever seulement des catégories suivantes :
a) — nom, nom marital, prénoms, adresse, numéro de téléphone, code interne de traitement permettant l'identification du locataire ou du candidat à la location et, le cas échéant, de sa caution, de l'acquéreur ou du candidat à l'acquisition, du copropriétaire ou du propriétaire, de l'associé (à l'exclusion du numéro d'inscription au répertoire national d'identification) ;
— état civil complet, date et lieu de naissance, nationalité du copropriétaire, du propriétaire de son conjoint si il a des droits dans la copropriété, de chacun des coindivisaires en cas d'indivision, du ou des titulaires des droits visés à l'article 6 du décret du 17 mars 1967 ;
— coordonnées du mandataire commun en cas d'indivision ou du gérant qui gère les lots.
b) identité bancaire ou postale ;
c) situation familiale et, le cas échéant, composition du foyer du candidat à la location et situation familiale du locataire ;
d) situation professionnelle, coordonnées de l'employeur du candidat à la location et du locataire ;
e) ressources du candidat à la location, du locataire, et, le cas échéant, de sa caution ;
f) logement : caractéristiques du logement ou des biens immobiliers, conditions de location ou d'accession à la propriété, date d'entrée et de départ, montant du dépôt de garantie, calcul du droit de bail, montant du loyer, nature et montant des charges, des travaux d'entretien et d'amélioration et nature des prêts consentis et des modalités de remboursement, compagnie d'assurance, numéro de police du locataire ;
g) numéro d'inscription à la caisse d'allocation familiale du bénéficiaire exclusivement pour permettre le versement de l'aide personnalisée au logement ;
h) disponibilités financières du candidat à l'acquisition d'un bien immobilier.

Article 4
Durée de conservation

Les informations nécessaires aux traitements automatisés d'informatisations nominatives définies aux articles 1, 2 et 3 ne doivent pas être conservées après le règlement du solde de l'intéressé ou la rupture de la relation contrac-

tuelle à l'exception des informations nécessaires à l'accomplissement des obligations légales.

Les informations relatives au candidat à la location ne peuvent être conservées que si la location est effectivement réalisée. A défaut de location, ces informations doivent être supprimées en cas de non-renouvellement de la demande dans un délai de 3 mois.

Article 5
Destinataires des informations

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des informations les concernant :
— les services chargés de la gestion et de la comptabilité des immeubles ;
— l'organisme financier teneur du compte du locataire, de l'accédant ou du propriétaire ;
— les auxiliaires de justice et les officiers ministériels dans le cadre de leur mission de recouvrement de créances ;
— les services publics, exclusivement pour répondre aux obligations légales.

Article 6

La norme simplifiée instituée par la délibération n° 81-54 du 26 mai 1981 est abrogée.

Délibération n° 99-059 du 9 décembre 1999 portant adoption du rapport et des recommandations relatifs aux modalités d'informatisation de la surveillance épidémiologique du sida et en particulier de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine

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

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° 98-535 du 1er juillet 1998 relative au renforcement de la veille sanitaire et du contrôle de la sécurité sanitaire des produits destinés à l'homme ;

Vu les décrets n° 99-362 et 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 les modalités de cette transmission ;

Après avoir entendu Monsieur Raymond FORNI, en son rapport, et Madame Charlotte-Marie PITRAT, Commissaire du gouvernement, en ses observations ;

Considérant que, par le décret nº 99-363 du 6 mai 1999, les pouvoirs publics ont souhaité inscrire sur la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire, l'infection par le virus de l'immunodéficience humaine, quel que soit le stade de la maladie ;

Considérant que les conditions dans lesquelles seront collectées et traitées à des fins de surveillance épidémiologique les informations relatives aux personnes séropositives, nécessitent que soient conciliés les impératifs de santé publique et le respect de la vie privée ;

Considérant que, dans ce souci, et en application de l'article 1er du décret du 17 juillet 1978, la Commission, après avoir entrepris des auditions auprès des associations de défense des malades atteints du sida, de la Ligue des droits de l'Homme et du Conseil national de l'Ordre des médecins, effectué des visites auprès de médecins inspecteurs des Directions départementales de l'action sanitaire et sociale et avoir tenu étroitement informé l'Institut de Veille Sanitaire, émet un certain nombre de recommandations sur les modalités de l'informatisation de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine ;

Décide :

— d'adopter le rapport et les recommandations relatifs aux modalités d'informatisation de la surveillance épidémiologique du sida et en particulier de la déclaration obligatoire de séropositivité au virus de l'immunodéficience humaine annexé à la présente délibération ;

— d'adresser ce rapport aux pouvoirs publics et organismes et associations concernés ;

— de publier ce rapport sur le site internet de la CNIL.

Décisions des juridictions

ARRÊT DU CONSEIL D'ÉTAT DU 14 JUIN 1999, SECTION DU CONTENTIEUX

Vu la requête enregistrée le 3 juillet 1998 au secrétariat du Contentieux du Conseil d'Etat, présentée par la société de traitement de visite médicale et de fichiers médicaux (TVF), dont le siège est 127, rue d'Aguessau à Boulogne-Billancourt (92103), représentée par son gérant ; la société TVF demande que le Conseil d'Etat :
1°) annule la délibération de la commission nationale de l'informatique et des libertés n° 98-045 du 12 mai 1998 portant avertissement à la société Publimed et à la société TVF ;
2°) condamne la commission nationale de l'informatique et des libertés à lui verser la somme de 30 000 F, en application de l'article 75 de la loi n° 91-647 du 10 juillet 1991 ;

Vu les autres pièces du dossier ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu la loi n° 91-647 du 10 juillet 1991 ;

Vu la délibération n° 87-25 du 10 février 1987 fixant le règlement intérieur de la commission nationale de l'informatique et des libertés ;

Vu l'ordonnance n° 45-1708 du 31 juillet 1945, le décret n° 53-934 du 30 septembre 1953 et la loi n° 87-1127 du 31 décembre 1987 ;

[...]

Sur les conclusions tendant à l'annulation de la délibération de la commission nationale de l'informatique et des libertés, en date du 12 mai 1998 :

Considérant qu'en vertu des dispositions de l'article 6 de la loi du 6 janvier 1978 susvisée, la commission nationale de l'informatique et des libertés est chargée de veiller au respect de ladite loi et qu'aux termes des dispositions de l'article 21-4° de la même loi, elle « adresse aux intéressés des avertissements », à cette fin ;

Considérant qu'il résulte de ces dispositions que, contrairement à ce qu'affirme la société requérante, la commission nationale de l'informatique et des libertés était compétente pour adresser, par la délibération attaquée, un avertissement à ladite société par lequel elle lui demandait de prendre toutes les dispositions nécessaires afin que M. B. obtienne, en application de la loi susmentionnée, les informations le concernant détenues par elle ;

Considérant, en deuxième lieu, qu'aux termes de l'article 56 de la délibération de la commission nationale de l'informatique et des libertés, en date du 10 février 1997, fixant son règlement intérieur : « Les missions d'investigation, de contrôle ou de vérification sont décidées par une délibération de la commission qui précise les missions et les commissaires ou les agents de la commission chargés de la mission décidée par la commission. La délibération est notifiée aux personnes concernées » ; que dès lors que la délibération du 4 novembre 1997 par laquelle la commission nationale a décidé une vérification sur place auprès de la société Publimed et de la société TVF désignait un commissaire chargé de cette mission, elle n'était pas tenue de désigner elle-même les agents chargés de l'assister ; que, par suite, le moyen tiré de ce que la procédure aurait été rendue irrégulière du fait de la désignation de ces agents par le président de la commission et non par la commission elle-même doit être écarté ;

Considérant, en troisième lieu, qu'aux termes des dispositions de l'article 34 de la loi du 6 janvier 1978 susvisée : « Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication » ; et qu'aux termes des dispositions de l'article 4 de la même loi : « Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale » ;

Considérant que M. B., visiteur médical, avait demandé à la société TVF des informations portant sur le nombre de visites quotidiennes qu'il avait effectuées auprès des médecins, au cours de la période allant du 1er septembre 1992 au 30 juillet 1994 ; qu'il s'agissait d'informations nominatives le concernant, au sens des dispositions précitées de l'article 4 de la loi du 6 janvier 1978 ; qu'il ressort, en outre, des pièces du dossier, et notamment des résultats de la vérification sur place qu'avait décidée la commission nationale, en application des dispositions du 2° de l'article 21 de la loi du 6 janvier 1978, que la société TVF détenait bienlesdites informations, à la date à laquelle M. B. les lui avait demandées ; que M. B. était en droit d'adresser sa demande d'accès soit auprès de la société Publimed, qui employait l'intéressé, soit à la société TVF, à laquelle la mise en œuvre du traitement automatisé avait été confiée en vertu d'un contrat de prestation de service passé avec la société Publimed, sans que la clause de confidentialité figurant dans la convention entre ces deux sociétés puisse lui être opposée ; qu'ainsi, en demandant, par la délibération attaquée, à la société TVF, de prendre toutes les dispositions nécessaires, afin que M. B. obtienne les informations le concernant détenues par ladite société, ce qui n'imposait pas la communication à M. B. d'informations nominatives concernant les médecins visités, la commission nationale a fait une exacte application des dispositions de la loi du 6 janvier 1978 ;

Sur les conclusions tendant à l'application des dispositions de l'article 75-I de la loi du 10 juillet 1991 :

Considérant que les dispositions de l'article 75-I de la loi du 10 juillet 1991 font obstacle à ce que la commission nationale de l'informatique et des libertés qui n'est pas, dans la présente instance, la partie perdante, soit condamnée à payer à la société TVF la somme qu'elle demande, au titre des frais exposés par elle et non compris dans les dépens ;

Décide :

Article 1er : La requête de la société TVF est rejetée.

Article 2 : La présente décision sera notifiée à la société TVF, à la commission nationale de l'informatique et des libertés et au Premier ministre.

ARRÊT DU CONSEIL D'ETAT DU 27 OCTOBRE 1999, SECTION DU CONTENTIEUX

Vu, la requête enregistrée au secrétariat du contentieux du Conseil d'Etat le 5 mai 1998, l'ordonnance en date du 28 avril 1998 par laquelle le président du tribunal administratif de Paris a transmis au Conseil d'Etat, en application de l'article R 81 du code des tribunaux administratifs et des cours administratives d'appel, la demande présentée à ce tribunal par M. S. ;

Vu la demande enregistrée au greffe du tribunal administratif de Paris le 28 juillet 1994, présentée par M. S., et tendant à l'annulation de la décision implicite par laquelle la Commission nationale de l'informatique et des libertés (CNIL) a refusé de transmettre au procureur de la République sa plainte relative au fonctionnement de la bibliothèque municipale de Bordeaux et a refusé de l'informer de la suite réservée à ladite plainte ;

Vu les autres pièces du dossier ;

Vu le code de procédure pénale et notamment son article 40 ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu la délibération n° 87-25 du 10 février 1987 fixant le réglement intérieur de la commission nationale de l'informatique et des libertés ;

Vu le code des tribunaux administratifs et des cours administratives d'appel ;

Vu l'ordonnance n° 45-1708 du 31 juillet 1945, le décret n° 53-934 du 30 septembre 1953 et la loi n° 87-1127 du 31 décembre 1987 ;

[...]

Sans qu'il soit besoin de statuer sur la fin de non-recevoir opposée par la commission nationale de l'informatique et des libertés :

Sur les conclusions dirigées contre la décision implicite par laquelle la commission nationale de l'informatique et des libertés a refusé de transmettre au procureur de la République la plainte de M. S. :

Considérant qu'aux termes de l'article 21 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « — Pour l'exercice de sa mission de contrôle, la commission : 4° 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 ; 6° reçoit les réclamations, pétitions et plaintes ; » ; qu'aux termes de l'article 40 du code de procédure pénale « Toute autorité constituée, ou officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs » ;

Considérant qu'en vertu de ces dispositions, il appartient à la commission nationale de l'informatique et des libertés d'aviser le procureur de la République des faits dont elle a connaissance dans l'exercice de ses attributions, si ces faits lui paraissent suffisamment établis et si elle estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application ;

Considérant que par des courriers en date des 2 et 22 janvier 1992, M. S. a saisi la commission nationale de l'informatique et des libertés du fait que la bibliothèque centrale municipale de Bordeaux n'informait pas ses usagers de ce que les informations relatives aux prêts de livres faisaient l'objet d'un traitement automatisé et ainsi ne les mettait pas en mesure d'exercer le droit d'accès et de rectification prévu par l'article 27 de la loi précitée du 6 janvier 1978 ; que, toutefois, la commission nationale de l'informatique et des libertés a immédiatement saisi le conservateur de la bibliothèque centrale municipale qui, alors que le traitement informatisé était en cours de mise en œuvre, a opéré les régularisations exigées et déclaré le traitement dans les conditions prévues par l'article 17 de la loi du 6 janvier 1978 ; que, dans ces conditions, la commission a pu, sans commettre d'erreur de droit ni d'erreur manifeste d'appréciation, estimer que les infractions invoquées par M. S. n'étaient pas suffisamment établies et ne portaient pas une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application pour justifier une trans-

mission au parquet dans les conditions prévues par l'article 21 de la loi du 6 janvier 1978 et l'article 40 du code de procédure pénal ; que M. S. n'est dès lors pas fondé à demander l'annulation, pour excès de pouvoir de la décision attaquée ;

Sur les conclusions dirigées contre le refus d'informer M. S. de la suite réservée à sa plainte :

Considérant que si les dispositions de l'article 54 de la délibération du 10 février 1987 précisent que le plaignant est tenu informé des suites réservées à sa plainte, la commission nationale de l'informatique et des libertés a satisfait ultérieurement à cette exigence ; que les conclusions susanalysées de M. S., sont dès lors devenues sans objet ;

Décide :

Article 1er : Il n'y a pas lieu à statuer sur les conclusions dirigées contre le refus d'informer M. S. de la suite réservée à sa plainte.

Article 2 : Le surplus des conclusions de la requête de M. S. est rejeté.

Article 3 : La présente décision sera notifiée à M. S., à la commission nationale de l'informatique et des libertés et au Premier ministre.

ARRÊT DU CONSEIL D'ETAT DU 3 DÉCEMBRE 1999, SECTION DU CONTENTIEUX

Vu 1°), sous le n° 197060, la requête enregistrée le 8 juin 1998 au secrétariat du Contentieux du Conseil d'Etat, présentée par la Caisse de crédit mutuel de Bain-Tresbœuf, dont le siège est 9, rue du Général Chassereau à Bain-de-Bretagne (35470), représentée par son président ; la Caisse de crédit mutuel de Bain-Tresbœuf demande que le Conseil d'Etat :
— annule la délibération, en date du 7 avril 1998, portant avertissement, de la Commission nationale de l'informatique et des libertés ;
— condamne la commission nationale à lui verser la somme de 30 000 F au titre de l'article 75-I de la loi du 10 juillet 1991 ;

Vu 2°), sous le n° 197061, la requête enregistrée le 8 juin 1998 au secrétariat du Contentieux du Conseil d'Etat, présentée par le GIE Federal Service, dont le siège est 32, rue Mirabeau à Le Relecq-Kerhuon (29480), représenté par son directeur ; le GIE Federal Service demande que le Conseil d'Etat :
— annule la délibération, en date du 7 avril 1998, portant avertissement, de la Commission nationale de l'informatique et des libertés ;
— condamne la commission nationale à lui verser la somme de 30 000 F au titre de l'article 75-I de la loi du 10 juillet 1991 ;

Vu les autres pièces des dossiers ;

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

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu la loi n° 91-647 du 10 juillet 1991 ;

Vu l'ordonnance n° 45-1708 du 31 juillet 1945, le décret n° 53-934 du 30 septembre 1953 et la loi n° 87-1127 du 31 décembre 1987 ;

[...]

Considérant que la requête n° 197060 présentée par la Caisse de crédit mutuel de Bain-Tresbœuf et la requête n° 197061 présentée par le GIE Federal Service sont dirigées contre la même délibération de la Commission nationale de l'informa-

tique et des libertés, en date du 7 avril 1998 ; qu'il y a lieu de les joindre pour statuer par une même décision ;

Considérant qu'aux termes de l'article 5 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives » ; qu'aux termes de l'article 6 de la même loi : « Une Commission nationale de l'informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique aux traitements des informations nominatives » ; qu'aux termes de l'article 21 de la même loi : « Pour l'exercice de la mission de contrôle, la commission : 1° prend des décisions individuelles ou réglementaires dans les cas prévus par la présente loi ; 2° peut, par décision particulière, charger un ou plusieurs de ses membres ou de ses agents, de procéder, à l'égard de tout traitement, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission ; 4° 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 ; 6° reçoit les réclamations, pétitions et plaintes ; » ;

Considérant que la Commission nationale de l'informatique et des libertés qui avait été saisie par des clients de la Caisse de Crédit Mutuel de Bain-Tresbœuf a fait procéder, par celui de ses membres qu'elle avait désigné comme rapporteur de cette plainte et par certains de ses agents, à une vérification sur place des traitements automatisés du fichier des clients de cette caisse ; qu'à la suite de cette vérification la Commission nationale de l'informatique et des libertés, par la décision attaquée du 7 avril 1998, a rappelé à la caisse les règles relatives aux informations nominatives, lui a demandé de procéder dans un délai d'un mois à l'effacement des informations contraires à ces règles et, faisant application du 4° de l'article 21 de la loi du 6 janvier 1978, lui a adressé un avertissement ;

Sur les moyens tirés de ce que le rapporteur a participé à l'adoption de la décision attaquée :

Considérant, d'une part, que la décision attaquée n'émane pas d'un tribunal au sens de l'article 6-1 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; qu'ainsi les requérants ne sont pas fondés à invoquer la méconnaissance de ces stipulations ;

Considérant, d'autre part, que la participation du rapporteur au débat et au vote qui ont conduit à l'adoption de la délibération attaquée n'a constitué une méconnaissance ni du principe d'impartialité ni de celui des droits de la défense ;

Sur les autres moyens :

Considérant qu'après que la Commission nationale de l'informatique et des libertés lui eut donné communication tant de la plainte dont elle avait été saisie que de sa décision de procéder à une vérification sur place en application du 2° de l'article 21 précité de la loi du 6 janvier 1978, la Caisse de crédit mutuel de Bain-Tresbœuf a informé la commission nationale de ce que le traitement des dossiers de son fichier était assuré de façon centralisée, au niveau régional, par le GIE Federal Service ; qu'il ressort, en outre, des pièces du dossier que la déclaration du fichier au-

près de la commission nationale avait été faite par la Caisse régionale de Crédit Mutuel de Bretagne ; que, par suite, alors même que la notification des griefs de la plainte et celle de la décision de la commission nationale de procéder à une vérification sur place n'avaient été adressées qu'à la caisse locale, la circonstance que cette vérification a eu lieu aussi au siège du GIE Federal Service, qui en avait été prévenu préalablement, n'a pas entaché la procédure d'irrégularité ;

Considérant qu'il ressort des pièces du dossier que les requérants ont eu connaissance des griefs qui leur étaient faits ainsi que du compte-rendu de la vérification sur place et qu'ils ont fait connaître leurs observations préalablement à la délibération attaquée ; qu'ils n'ont pas demandé à être entendus, comme le permettait le règlement intérieur de la commission nationale ; qu'aucune disposition n'imposait la communication préalable du rapport présenté à la commission ; qu'ainsi les moyens tirés de ce que le principe du caractère contradictoire de la procédure n'aurait pas été respecté ne peuvent être accueillis ;

Considérant que les données contenues dans la zone « bloc-notes » du fichier des clients de la Caisse de crédit mutuel de bain-Tresbœuf, géré de façon centralisée par le GIE Federal Service, faisaient l'objet d'un traitement automatisé d'informations nominatives, au sens des dispositions de l'article 5 précité de la loi du 6 janvier 1978 ; que la commission nationale n'a pas méconnu ces dispositions en demandant à la caisse, par la délibération attaquée portant avertissement, de procéder à l'effacement de celles des informations nominatives qui n'étaient pas « pertinentes, adéquates et non-excessives » au regard de la finalité du traitement ; Considérant que les modalités selon lesquelles la délibération attaquée a été notifiée ou portée à la connaissance de la presse sont sans incidence sur sa légalité ;

Sur les conclusions tendant à l'application des dispositions de l'article 75-I de la loi du 10 juillet 1991 :

Considérant que les dispositions de l'article 75-I de la loi du 10 juillet 1991 font obstacle à ce que l'Etat, qui n'est pas, dans la présente instance, la partie perdante, soit condamné à payer aux requérants les sommes qu'ils demandent au titre des frais exposés par eux et non compris dans les dépens ;

Décide :

Article 1er : Les requêtes de la Caisse de crédit mutuel de Bain-Tresbœuf et du GIE Federal Service sont rejetées.

Article 2 : La présente décision sera notifiée à la Caisse de crédit mutuel de Bain-Tresbœuf, au GIE Federal Service, à la Commission nationale de l'informatique et des libertés et au Premier ministre.

Actualité parlementaire

CNIL

Modification de la loi « informatique et libertés »

11883 — 23 mars 1998. — **M. Léonce Deprez** demande à **Mme le garde des sceaux, ministre de la justice** de lui préciser la suite qu'elle envisage de réserver aux propositions du récent rapport « Données personnelles et société de l'information », récemment remis au Premier ministre. Ce rapport, évoquant l'adaptation de la loi « Informatique et libertés » (janvier 1978), propose notamment que la Commission nationale informatique et libertés (CNIL) puisse disposer de réels pouvoirs d'enquête sur les organismes disposant de fichiers, prendre toute mesure conservatoire utile pour faire cesser le traitement illégal ou non conforme de données. Ce rapport souhaite également une clarification des relations entre les parquets et la CNIL, la CNIL pouvant disposer du droit de se constituer partie civile en cas de manquements manifestes à la législation. S'agissant des libertés fondamentales des Français, il lui demande la suite concrète qu'elle envisage de réserver à ces propositions, qui avait d'ailleurs largement inspiré un rapport remis, le 17 novembre 1996, à son prédécesseur, et dont ses services sont bien informés.

Réponse. — Le garde des sceaux, ministre de la justice, fait connaître à l'honorable parlementaire que le rapport intitulé *Données personnelles et société de l'information,* remis au Premier ministre le 3 mars 1998 par M. Guy Braibant, propose de renforcer substantiellement les prérogatives de la Commission nationale de l'informatique et des libertés (C.N.I.L.) en matière de contrôle *a posteriori* de traitements de données à caractère personnel. Conformément à ces propositions, il est envisagé de confier aux agents de la Commission des pouvoirs d'enquête, en leur permettant notamment de procéder à des visites et à des saisies dans des conditions similaires à celles prévues pour d'autres autorités administratives indépendantes, telles le Conseil de la concurrence ou la Commission des opérations de bourse, l'exercice de ces pouvoirs étant toutefois soumis à une autorisation judiciaire au cas par cas, afin de respecter la jurisprudence du Conseil constitutionnel. Par ailleurs, les services de la chancellerie étudient les modalités exactes selon lesquelles l'autorité de protection pourrait être dotée d'un pouvoir général d'enjoindre les mesures appropriées pour faire cesser les atteintes graves aux droits fondamentaux des personnes et, si ses injonctions ne sont pas suivies d'effet, de saisir le juge afin de voir ordonner par celui-ci, — le cas échéant sous astreinte, ces mesures. S'agissant plus particulièrement du pouvoir d'agir devant le juge pénal, le rapport élaboré par M. Guy Braibant a estimé inopportune une remise en cause du principe selon lequel il appartient au ministère public de mettre en mouvement l'action publique. Il propose, en conséquence, soit de conférer à la C.N.I.L. le pouvoir de se constituer partie civile incidente, soit de lui permettre, sans être partie à l'instance, de présenter des observations écrites et orales dans les procédures pénales. Cette seconde solution, qui paraît la plus adéquate, devrait être privilégiée dans le projet de réforme actuellement en cours de finalisation.

Assemblée nationale 15 mars 1999 n° 11 (p. 1605)

11890 — 23 mars 1998. — **M. Léonce Deprez** demande à **M. le Premier ministre** de lui préciser la suite qu il envisage de réserver au rapport qui lui a été récemment remis : « Données personnelles et société de l'information », tendant à proposer de nombreuses a importantes adaptations de la loi Informatique et libertés

(janvier 1978). Il lui demande notamment de lui préciser s'il envisage, comme le propose ce rapport, de renforcer les pouvoirs de la Commission nationale Informatique et libertés (CNIL), notamment — par une ouverture aux membres du secteur privé et la déconcentration de ses services par le biais de la création d'antennes régionales. — **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 les suites apportés au rapport remis au Premier ministre par M. Guy Braibant le 3 mars 1998 et, notamment, le renforcement substantiel que celui-ci préconise des prérogatives de la Commission nationale de l'informatique et des libertés (C.N.I.L.) dans le contrôle a posteriori des traitements, seront mises en œuvre dans le cadre du projet de loi, actuellement en cours de finalisation par la Chancellerie, qui assurera la transposition de la directive communautaire du 24 octobre 1995 relative à la protection des personnes à 1'égard du traitement de données à caractère personnel. Dans le régime issu de cette transposition, les contrôles préalables exercés par la C.N.I.L se trouveront circonscrits aux seules catégories de traitements présentant des risques d'atteinte aux droits des personnes, mais pourront concerner aussi bien les traitements à finalité privée que les traitements à finalité publique. S'il ne fait par ailleurs aucun doute que les nouvelles missions de la C.N.I.L. rendront indispensable un accroissement des moyens et des capacités d'expertise dont disposent ses services, les modalités que revêtira leur renforcement ne sont pas définitivement arrêtées.

Assemblée nationale, 22 février 1999 n° 8 (p. 1109)

24001 — 18 janvier 1999. — **M^me^ Marie-Jo Zimmermann** appelle l'attention de **M. le ministre de l'intérieur** sur les conditions d'accès des citoyens aux fichiers informatiques les concernant et recensés par la Commission nationale de l'informatique et des libertés. Il lui rappelle que l'article 3 de la loi du 6 janvier 1978 dispose' « que toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés ». Or, il semble que la CNIL organisme collecteur, ne soit pas en mesure, en raison du nombre très important de fichiers qu'elle détient, de communiquer directement aux particuliers qui en font la demande l'ensemble des fichiers les concernant. Il appartiendrait donc aux particuliers de s'adresser directement auprès des organismes ou administrations détenant des informations sur leur compte. Si comme la CNIL l'affirme, il existe bien 603 000 fichiers recensés la procédure de demande auprès de chacun des organismes concernés est quasiment impossible pour tout particulier. Il en résulte que le citoyen qui désire user de son droit de rectification ou de suppression d'informations le touchant, tel qu'il est prévu à l'article 36 de la loi du 6 janvier 1978, ne dispose d'aucun moyen réel pour le faire. Aussi, elle lui demande quelles mesures il entend prendre pour que tout citoyen ait les moyens matériels d'exercer son droit de regard sur des informations le concernant, conformément aux termes des articles 3 et 36 de la loi susvisée. — **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 qu'il est exact que la possibilité pour les citoyens d'avoir effectivement accès aux indications qui les concernent dans la liste des traitements d'informations nominatives, tenue par la Commission nationale de l'informatique et des libertés (CNIL), en vertu de l'article 22 de la loi du 6 janvier 1978 relative à 1'informatique aux fichiers et aux libertés, se heurte à des obstacles pratiques. Outre le nombre considérable de fichiers et celui des traitements du secteur privé qui ont échappé à la formalité de déclaration préalable prévue par l'article 16 de la loi susvisée, doit être soulignée l'absence de paramètres permettant à un requérant, même

avec l'aide de la CNIL d'identifier avec certitude les caractéristiques du ou des traitements dont il cherche à obtenir confirmation de l'existence ou de la régularité. Toutefois, il n'est envisagé, dans le cadre du projet de loi de transposition de la directive communautaire du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, ni de soumettre à une obligation déclarative, à l'instar du régime actuel, l'ensemble des traitements ne faisant pas l'objet d'une autorisation préalable, ni de reprendre l'obligation incombant actuellement à la CNIL de tenir une liste exhaustive des traitements. En effet, il n'apparaît pas que l'existence et 1'accessibilité d'une telle liste soient, au regard de la directive de 1995. un préalable nécessaire à l'exercice par toute personne de son droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés, ainsi que de ses droits d'opposition au traitement et d'accès et de rectification aux données personnelles de l'intéressé qu'il comporte. Le rapport Braibant a estimé pour sa part qu'il était préférable, dans l'intérêt même des libertés et des droits le l'homme, que la CNIL consacre ses efforts, plutôt qu'à un dénombrement a priori des traitements, dont l'exhaustivité et l'intérêt sont hautement problématiques, à la surveillance de ceux d'entre eux qui apparaissent potentiellement dangereux, ou dont la mise en œuvre s'avère, après coup, génératrice d'une atteinte aux droits et libertés. Il a par ailleurs préconisé un renforcement important des pouvoirs de contrôle a posteriori dont dispose la CNIL. Cette dernière orientation sera très largement suivie, le texte préparé par le Gouvernement reconnaissant à l'autorité de protection créée en 1978 des pouvoirs d'investigation et de sanction substantiellement accrus, propres à garantir les droits fondamentaux des personnes à l'égard du traitement des données les concernant et ce, conformément aux souhaits exprimés par l'auteur de la question.

Assemblée nationale, 24 mai 1999 n° 21 (p. 3183)

7281 — 2 avril 1998. — **M. Serge Mathieu** demande à **M. le Premier ministre** de lui préciser la suite qu'il envisage de réserver au rapport qui lui a été récemment remis : « Données personnelles et société de l'information », tendant à proposer de nombreuses et l'importantes adaptations de la loi Informatique et libertés (janvier 1978). Il lui demande notamment de lui préciser s'il envisage, comme le propose ce rapport, de renforcer les pouvoirs de la Commission nationale informatique et libertés (CNIL), notamment par une ouverture aux membres du secteur privé et la déconcentration de ses services par le biais de la création d'antennes régionales. — **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 les suites apportées au rapport remis au Premier ministre par M. Guy Braibant le 3 mars 1998 ce, notamment, le renforcement substantiel que celui-ci préconise des prérogatives de la Commission nationale de l'informatique et des libertés (CNIL) dans le contrôle a posteriori des traitements seront mis en œuvre dans le cadre du projet de loi, actuellement en cours de finalisation par la chancellerie, qui assurera la transposition de la directive communautaire du 24 octobre 1995 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Dans le régime issu de cette transposition, les contrôles préalables exercés par la CNIL se trouveront circonscrits aux seules catégories de traitement présentant —, des risques d'atteintes aux droits des personnes, mais pourront concerner aussi bien les traitements à finalité privée que les traitements à finalité publique. S'il ne fait, par ailleurs, aucun doute que les nouvelles missions de la CNIL rendront indispensable un accroissement des moyens et des capacités d'expertise

dont disposent ses services, les modalités que revêtira leur renforcement ne sont pas définitivement arrêtées.

Sénat, 25 février 1999 n° 8 (p. 625)

ÉCONOMIE

Fichiers de clients et chèques

12699 — 10 décembre 1998. — **M. Jacques Peyrat** appelle l'attention de **M. le ministre de l'intérieur** sur l'application de la loi n° 78-17 informatique et liberté du 6 janvier 1978. En effet, de nombreux commerçants constituent aujourd'hui des fichiers de clients (nom, prénom, adresse) grâce aux chèques qu'ils reçoivent. Il s'avère que, bien souvent, ces listes sont ensuite cédées ou échangées, ce qui est parfaitement inacceptable. De plus, les commerçants prétendent agir en route légalité dès lors que les personnes concernées ne se sont pas opposées préalablement à la constitution de ces fichiers. En conséquence, il lui demande ce que lui inspire cette pratique et s'il compte prendre des mesures pour la faire cesser. — **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 loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, si elle n'a pas entendu prohiber la constitution par les entreprises de fichiers de clientèle et leur cession ultérieure éventuelle à des tiers, a subordonné la licéité de telles utilisations commerciales des informations nominatives à des principes destinés à garantir la loyauté de la collecte des données. Ainsi, en vertu des articles 26 et 27 de la loi susvisée, les auteurs d'une collecte de données ont ils l'obligation d'informer les personnes auprès desquelles celles-ci sont recueillies, notamment de ce que des tiers peuvent en être destinataires dans le cadre d'une cession par leurs détenteurs des fichiers correspondants. Dès lors, les intéressés ont la faculté, avant même la mise en œuvre de la cession, de s'opposer soit à toute collecte des données les concernant, soit à la modalité particulière du traitement de celles-ci que constitue leur mise à la disposition d'un tiers. Un non-respect de cette obligation d'information comme du droit d'opposition que celle-ci permet aux personnes d'exercer est pénalement sanctionné. En outre dès lors qu'ils revêtent la forme d'un traitement automatisé, les fichiers de clientèle sont, à l'instar de tout autre fichier informatisé, soumis à l'une des formalités prévues par les articles 15 et 16 ; de la loi du 6 janvier 1978, celles-ci supposant que tout objet de cession du fichier à des tiers soit porté à la connaissance de la Commission nationale de l'informatique et des libertés (CNIL) dans le cadre de la demande d'avis ou de la déclaration qui lui est adressée. Toutefois, même si le principe de loyauté de la collecte des données paraît devoir appeler une information générale des intéressés, la question de savoir si l'article 27 de la loi susvisée, qui régit spécifiquement les situations de recueil direct des données auprès de personnes que celles-ci concernent, est applicable à l'hypothèse à laquelle fait référence l'auteur de la question n'a pas été tranchée à ce jour par la jurisprudence. Il est envisagé de remédier à cette lacune des textes dans le cadre du projet de loi de transposition de la directive du 24 octobre 199S relative à la protection et à la libre circulation de ces données. Ce texte communautaire prévoit en effet une extension de l'obligation d'information du maître d'un fichier à toute forme de collecte de données, que celle-ci soir directe ou indirecte. Il conduira par ailleurs le Gouvernement à conférer un caractère discrétionnaire au droit des personnes de s'opposer à un traitement répondant à une finalité de prospection, notamment commerciale, alors qu'un tel droit est subordonné sous le régime actuel à l'existence d'une raison légitime. Il permettra enfin, grâce à l'augmentation substantielle des

pouvoirs d'investigation et de sanction dont dispose la CNIL, un contrôle plus effectif des conditions juridiques dans lesquelles ont lieu les opérations de cession de fichiers, eu égard à leur transparence, ainsi qu'une prévention plus efficace des manquements du responsable du traitement à ses obligations.

Sénat 17 juin 1999 n° 24 (p. 2075)

FISCALITÉ

Utilisation du NIR

30885 — 7 juin 1999. — **M. Jean Rouger** souhaite attirer l'attention de **M. le ministre de l'économie, des finances et de l'industrie** sur le système NIR. Suite à l'adoption, dans le cadre des discussions du projet de loi de finances 1999, de diverses dispositions destinées à lutter contre la fraude fiscale, les administrations financières sont désormais autorisées à utiliser le numéro d'inscription au répertoire national (NIR). Force est de constater, même s'il ne s'agit en aucun cas de remettre en cause la lutte contre la fraude fiscale, que ces mesures ont suscité une vive émotion à la commission nationale Informatique et libertés. Son président, M. Fauvet, a d'ailleurs rappelé, à cette occasion, que « ces dispositions faciliteraient des transferts d'informations à l'insu des intéressés, y compris au bénéfice d'organismes tiers déclarants, comme les banques et les compagnies d'assurances ». C'est la raison pour laquelle il lui demande si ces mesures ne sont pas de nature à accentuer le caractère exorbitant des prérogatives de l'administration fiscale, et si elles ne représentent donc pas, par conséquent, un risque de fichage potentiel pour nos concitoyens.

Réponse. — La Commission nationale informatique et libertés a rendu le 24 juin 1999 un avis favorable au projet de décret en Conseil d'état pris pour l'application de l'article 107 de la loi de finances pour 1999, précisant le dispositif d'utilisation du numéro d'inscription au répertoire national (NIR) par les administrations financières. Ces dernières utiliseront le numéro NIR dans leurs relations avec les organismes sociaux et les seuls tiers déclarants déjà autorisés à en disposer et pour fiabiliser l'identifiant national SPI dont elles se serviront dorénavant dans les relations directes usuelles avec les contribuables. Les conditions et objectifs d'utilisation du NIR et les garanties mises en œuvre sont pleinement de nature à répondre aux préoccupations soulevées par le parlementaire quant à la préservation des libertés publiques.

Assemblée nationale 11 octobre 1999 n° 41 (p. 5879)

27513 — 29 mars 1999. — **M. Jean-Michel** attire l'attention de **M. le ministre de l'économie, des finances et de l'industrie** sur les dispositions contenues dans la loi de finances de 1999 relative à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques. Cette disposition entre dans le cadre de la lutte contre la fraude fiscale dont le montant semble progresser, au vu de la dernière étude rendue publique à ce sujet. L'amendement adopté trouve son origine dans les travaux effectués par la mission parlementaire sur l'évaluation des fraudes et pratiques abusives, ainsi que dans la mission d'information sur la fraude et l'évasion fiscales confiée à M. Brard, titulaire de l'amendement susvisé. Or le texte adopté par l'Assemblée dans la loi de finances dispose que les modalités d'application seront fixées par un décret en Conseil d'Etat pris après avis de la CNIL. S'agissant de lutte contre la fraude, il est certain que le décret susvisé doit intervenir dans les plus brefs délais. Il lui demande donc si le Conseil d'Etat a bien été saisi, ainsi que la CNIL, où en est la procédure permettant l'adoption et la publication du décret susvisé, et à quelle date celui-ci pourra enfin paraître.

Réponse. — Le projet de décret d'application de l'article 107 de la loi de finances pour 1999, qui autorise 1'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) par les administrations financières, a reçu un avis favorable de la Commission nationale de l'informatique et des libertés le 23 juin 1999. Il doit maintenant être examiné par le Conseil d'Etat. Tout est mis en œuvre pour qu'il soit publié le plus rapidement possible et que les fichiers des administrations fiscales puissent ainsi être fiabilisés grâce au NIR.

Assemblée nationale 2 août 1999 n° 31 (p. 4715)

INTERNET

Régulation

10318 — 20 août 1998. — **M. Georges Gruillot** appelle l'attention de **M. le Premier ministre** sur les enjeux juridiques liés à Internet, particulièrement mis en lumière par la mission interministérielle présidée par M^me^ Falque-Pierrotin et une jurisprudence nouvelle. Il le remercie de lui préciser les suites qu'il entend donner aux propositions du rapport cité et plus particulièrement si une réflexion d'ensemble est engagée sur les questions posées par Internet sur le plan juridique.

Réponse. — L'honorable parlementaire attire l'attention de monsieur le Premier ministre sur la question des enjeux juridiques liés au développement d'Internet. Conformément à ce qu'avait annoncé le Premier ministre à Hourtin, le 25 août 1997, le Conseil d'Etat a été chargé d'une réflexion sur les enjeux juridiques du développement d'Internet. Ce rapport sur Internet et le droit a été rendu public le 8 septembre dernier. Le comité interministériel pour la société de l'information, qui s'est tenu le 19 janvier 1999 sous la présidence du Premier ministre, a pris une série de décisions importantes qui prennent notamment en compte les propositions du Conseil d Etat. Ces décisions concernent : 1° La libéralisation complète de l'usage de la cryptologie. Face au développement des moyens d'espionnage électronique, la possibilité de crypter les communications apparaît comme une réponse efficace pour protéger la confidentialité des échanges et la vie privée. Le Gouvernement s'est donné le temps de la réflexion. Après avoir consulté les acteurs, les experts et ses partenaires internationaux, il a acquis la conviction que les dispositions issues de la loi de 1996 ne sont plus adaptées. Elles restreignent fortement l'usage de la cryptologie dans notre pays, sans pour autant permettre aux pouvoirs publics de lutter efficacement contre des agissements criminels dont le chiffrement pourrait faciliter la dissimulation. Elles font en outre apparaître un risque d'isolement de la France par rapport à ses principaux partenaires. Le Gouvernement a donc décidé un changement fondamental d'orientation, qui vise à rendre complètement libre l'usage de la cryptologie en France, tout en adaptant les moyens des pouvoirs publics pour garantir les libertés publiques dans ce nouvel environnement et pour lutter contre l'utilisation des moyens de chiffrement à des fins délictueuses. Le projet de réforme législative qui sera présenté au Parlement s'articulera autour des orientations suivantes : offrir une liberté complète dans l'utilisation des produits de cryptologie, sous la seule réserve du maintien des contrôles à l'exportation découlant des engagements internationaux de la France (moyens de chiffrements faisant appel à des clés d'une longueur supérieure à 56 bits) ; supprimer le caractère obligatoire du recours aux tierces parties de confiance pour le dépôt des clés de chiffrement. Le rôle de tiers de confiance ne sera pas limité à la gestion des dés mais pourra s'étendre à d'autres missions, comme la certification de signatures électroniques. Le recours à ces organes et aux mécanismes d'auto-séquestre sera encouragé. Les tiers de confiance pourront notamment solliciter l'attribution d'un label auprès des pouvoirs publics ; permettre aux pouvoirs publics de lutter efficace-

ment contre l'usage des procédés de chiffrement à des fins délictueuses. A cet effet, le dispositif juridique actuel sera complété par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés. De même, les capacités techniques des pouvoirs publics seront significativement renforcées. Une modification de la loi est donc nécessaire, ce qui prendra plusieurs mois. Mais le Gouvernement a voulu que les entraves qui pèsent sur les citoyens soucieux de protéger la confidentialité de leurs échanges et sur le développement du commerce électronique soient levées sans attendre. Ainsi, dans l'attente des modifications législatives annoncées, le Gouvernement a décidé de relever le seuil de la cryptologie, dont l'utilisation est libre, de 40 bits à 128 bits, niveau considéré par les experts comme assurant durablement une très grande sécurité. 2° La mise en place d'un haut niveau de protection des données personnelles. La transposition de la directive européenne de 1995 relative à la protection des données à caractère personnel doit permettre d'adapter le cadre juridique interne à la généralisation du traitement informatique des données et à l'essor d'Internet. Elle doit garantir la préservation des droits aussi fondamentaux que la liberté individuelle « le respect dû à la vie privée. La transposition de la directive, loin d'affaiblir les garanties légales aujourd'hui offertes aux citoyens, aura pour objet d'assurer à ceux-ci un haut niveau de protection. Dans cette optique, les orientations que le Gouvernement proposera viseront notamment au renforcement des moyens de la Commission nationale de l'informatique et des libertés (CNIL), de pouvoir de contrôle de la CNIL. En particulier, la CNIL devra être en mesure de mieux exercer son pouvoir de contrôle a posteriori dans le domaine, en expansion rapide, du traitement des données à des fins commerciales. 3° La levée des obstacles juridiques concernant les documents numériques et la signature électronique. Les transactions dématérialisées prennent une importance croissante, que ce soit en matière commerciale ou dans les procédures administratives. Certains obstacles juridiques rendent nécessaire une modification du code civil pour permettre l'adaptation de notre droit de la preuve aux nouvelles technologies et à la signature électronique. Cette modification répondra à une double préoccupation : la conformité avec les orientations retenues au sein de l'Union européenne ; la prise en compte, avec toutes les garanties nécessaires, de la valeur probante du document sous forme numérique et des signatures électroniques.

Sénat 18 février 1999 n° 7 (p. 513)

Données de connexion

17256 — 17 juin 1999. — **M. Emmanuel Hamel** attire l'attention de **M^me^ le garde des sceaux, ministre de la justice,** sur la suggestion faite à la page 16 de l'étude intitulée « Internet et les réseaux numériques » adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, d'imposer aux intermédiaires techniques des obligations de conservation des données de connexion « afin de faciliter les enquêtes judiciaires par une meilleure » traçabilité « des utilisateurs de réseaux ». Il lui demande quelle a été sa réaction face à cette suggestion et souhaiterait savoir quelle suite lui a été ou va lui être donnée.

Réponse. — Le garde des sceaux, ministre de la justice, souhaite tout d'abord rappeler à l'honorable parlementaire que le Gouvernement a fait connaître, publiquement et à de nombreuses reprises, son intention de mettre en place une réglementation d'ensemble encadrant le développement des nouvelles technologies de l'information et de la communication telles que les réseaux numériques de type Internet. Plusieurs textes de nature législative sont actuellement en voie d'élaboration. Peut être cité tout d'abord le projet de loi portant adaptation du droit de la preuve

aux technologies de l'information et relatif à la signature électronique qui sera bientôt soumis au Parlement. De même, l'avant-projet de loi assurant la transcription, en droit français, de la directive communautaire sur la protection des données personnelles, qui modifie la loi n° 78-17 du 6 janvier 1978 relative à 1'informatique, aux fichiers et aux libertés, sera transmis très bientôt à la Commission nationale de l'informatique et des libertés ainsi qu'à la Commission nationale consultative des droits de l'homme. En ce qui concerne la question sensible de la conservation des données de connexion, il faut tout d'abord constater que s'impose le principe de nécessité. En effet, cette conservation s'avère indispensable à une répression effective des infractions commises sur l'Internet ou par le biais de l'Internet. La traçabilité permise par les données de connexion est absolument nécessaire tout à la fois à l'identification des auteurs des infractions et à la détermination des éléments matériels de celles-ci. Il convient donc d'élaborer un dispositif légal permettant de concilier la protection de la vie privée, qui pourrait être mise à mal par une excessive durée de conservation des données de connexion, et l'intérêt social essentiel que constitue l'efficacité de la lutte contre la délinquance, qui impose que ne soient pas désarmées les autorisés judiciaires chargées de réprimer la cybercriminalité. Le Gouvernement poursuit sa réflexion sur ce sujet et soumettre des propositions à la représentation nationale dans le cadre du projet de loi sur la société de 1'informarion, qui fera suite à la consultation nationale engagée sur ce thème.

Sénat 9 décembre 1999 n° 48 (p. 4077)

LIBERTÉS PUBLIQUES

Multiplication de fichiers

23457 — 28 décembre 1998. — **M. Jean de Gaulle** attire l'attention de **M^me^ le garde des sceaux, ministre de la justice,** sur l'incidence de la création et de l'utilisation des fichiers informatiques sur le droit à la protection de la vie privée des citoyens. La multiplication de ces fichiers, tant au niveau du ministère des finances. avec la mise au point du système informatisé sur les avoirs des Français, qu'au niveau judiciaire, avec la connexion des fichiers de police des Etats européens, par exemple, permettent à la justice le croisement d'informations de sources différentes et d'analyser de manière plus approfondie le comportement des ménages et des individus. Devant cette prolifération d'informations, il lui demande quelles dispositions le Gouvernement compte prendre afin de garantir aux citoyens une meilleure protection des données les concernant.

Réponse. — Le garde des sceaux, ministre de la justice, fait connaître à l'honorable parlementaire que les possibilités d'interconnexions de fichiers d'informations de fichiers d'informations nominatives de l'administration sont soumises à des dispositions protectrices des droits et libertés des personnes qui excluent, en particulier, que les fichiers des administrations économiques et financières fassent l'objet d'un croisement avec des fichiers de police judiciaire ou avec des fichiers nominatifs, publics ou privés, destinés à établir des profils de comportement des ménages ou des individus. Ainsi, une interconnexion de deux fichiers informatiques de l'administration, quand bien même ces derniers auraient précédemment été régulièrement autorisés, constitue-t-elle un traitement automatisé d'informations nominatives au sens de l'article 5 de la loi du 6 janvier 1978 relative à 1'informatique, aux fichiers et aux libertés et appelle-t-elle à ce titre, en vertu de l'article 15 de celle-ci, une autorisation, qui, sauf cas où celle-ci relève du législateur, prend forme d'un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés (CNIL), cet acte étant nécessairement un décret pris sur avis conforme du Conseil

d'Etat si l'avis de la commission est défavorable. En outre, les interconnexions de fichiers administratifs actuellement admises en droit français obéissent, à l'instar de tout traitement de données nominatives, à des principes de spécification de leur finalité et de pertinence par rapport à celle-ci des données enregistrées au respect desquels la CNIL est particulièrement attentive. La directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, dont la France assurera prochainement la transposition, conduits à un régime circonscrivant aux seules catégories de traitements présentant des risques pour les droits et libertés des personnes les contrôles préalables opérés par la CNIL, mais étendant parallèlement ceux-ci aux traitements du secteur privé. Les modifications apportées à la loi susvisée du 6 janvier 1978 à 1'occasion de cette transposition seront par conséquent de nature à permettre une extension au secteur privé de garanties qui entourent dans le cadre des textes en vigueur les seules interconnexions de fichiers publics

Assemblée nationale 26 avril 1999 n° 17 (p. 2537)

Interconnexions

24605 — 1er février 1999. — **M. Alain Le Vern** attire l'attention de **M. le Premier ministre** sur les réactions de beaucoup de citoyens suite à l'interconnexion des fichiers de la sécurité sociale et de l'administration fiscale. Tout en reconnaissant l'utilité et l'efficacité des technologies nouvelles, il y a lieu de prendre garde à ne pas ouvrir la voie à la constitution d'un réseau de fichiers accessibles à toutes les administrations. L'éventuelle création d'un fichier concernant les personnes mises en cause dans des affaires pénales, sans être condamnées, inquiète également. Il lui demande quelles dispositions il compte prendre pour assurer le respect de la vie privée des citoyens.

Réponse. — L'article 5 de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en date du 28 janvier 1981, prévoit que les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être « enregistrées pour des finalités déterminées et légitimes et ne (doivent pas être) utilisées de manière incompatible avec ces finalités ». Cette disposition doit être rapprochée de l'article 20 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à 1'informatique, aux fichiers et aux libertés, aux termes duquel les actes réglementaires instituant des traitements automatisés d'informations nominatives opérés pour le compte de personnes publiques doivent préciser les finalités en vue desquelles les données sont collectées et conservées. Enfin, l'article 226-21 du code pénal punit d'une peine de cinq ans d'emprisonnement et de 2 MF d'amende « le fait, par toute personne détentrice d'informations nominatives (...) de détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatisé ». Ces dispositions sont de nature à faire obstacle à l'interconnexion généralisée des fichiers ou, comme l'indique l'honorable parlementaire, à « la constitution d'un réseau de fichiers accessibles à toutes les administrations ». L'interconnexion de fichiers publics n'est donc possible que si cela est prévu dans l'acte réglementaire les instituant, pris sous le contrôle de la CNIL, ou si une disposition législative l'autorise expressément. Lorsque le Conseil constitutionnel a examiné l'article 107 de la loi de finances pour 1999 (n° 98-1266 du 30 décembre 1998), qui a autorisé la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droit indirects à utiliser le numéro d'inscription au répertoire national d'identification des personnes physiques, et qui a précisé que lesdites directions pourraient mentionner ce numéro lorsqu'elles

communiquent, en application de l'article L. 152 du livre des procédures fiscales, des informations aux organismes de sécurité sociale, il a déclaré cette disposition conforme à la Constitution dans la mesure où elle avait pour seule finalité d'éviter des erreurs d'identité et ne conduisait nullement à la création de fichiers nominatifs sans rapport direct avec « les missions incombant aux différents services et organismes concernés (décision n° 98-405 DC du 29 décembre 1998). Le principe de finalité n'était, par conséquent, nullement mis en cause par la loi de finances. Le Parlement aura la possibilité de prendre à nouveau position sur ce sujet à l'occasion de la discussion du projet de loi assurant la transposition de la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dont la préparation est en cours. L'article 6 de cette directive s'inscrit dans la ligne des dispositions susmentionnés puisqu'il prévoit que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ». Le Gouvernement est naturellement attaché, à l'occasion de la transposition de cette directive, à maintenir le niveau des garanties offert actuellement par la loi.

Assemblée nationale 19 août 1999 n° 16 (p. 2324)

Réseau Echelon

22360 — 7 décembre 1998. — **M. Georges Sarre** attire l'attention de **M. le ministre des affaires étrangères** sur la réponse donnée le 2 novembre dernier à sa question écrite du 13 avril 1998 portant sur les activités du réseau Echelon de surveillance et d'interception globales des télécommunications à l'échelle mondiale, géré conjointement par les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Au-delà des précisions opportunément apportées par M. le ministre sur les actions nationales et internationales engagées « pour remédier aux possibilités d'utilisation préjudiciable des nouvelles technologies de l'information », il retient surtout de la réponse ministérielle que les activités du réseau Echelon « constituant un sujet de préoccupation pour le Gouvernement français », et que celui-ci « entend participer activement aux suites qui seront données à ce rapport ». Quant à la question centrale soulevée dans sa question écrite initiale — à savoir, la profonde implication dans la définition, la mise en œuvre et l'exploitation du réseau Echelon d'un de nos principaux partenaires de l'Union européenne, et de la situation particulièrement aiguë de conflit d'intérêts qui en découle —, force est de constater qu'il n'est même pas fait mention, dans la réponse ministérielle, d'une quelconque évocation précise du sujet avec nos partenaires britanniques. Tel est pourtant bien le nœud du problème, au fondement de la question écrite qu'il a posée au printemps dernier, ou bien doit-on comprendre que la question du réseau Echelon a été abordée au sein du G8 — où figurent trois des principaux opérateurs du réseau Echelon — ou de l'Union européenne ? Ces enceintes multilatérales ne discutent-elles pas pour l'heure précisément, comme l'indique la réponse ministérielle, de dispositions visant à « améliorer les capacités des services répressifs et judiciaires en matière d'enquête et de poursuites de la criminalité liée à l'utilisation des technologies de pointe mais aussi à définir les limites à l'action des services nationaux aux regard de la souveraineté de chaque Etat, de la protection des droits de l'homme, des libertés démocratiques et de la vie privée » ? Nous touchons bien ici, en effet, au cœur même des problématiques soulevées par le dossier Echelon. Dès lors, n'est-il pas illusoire d'attendre de ceux-là même qui espionnent quotidiennement nos administrations, nos organisations et nos entreprises la définition d'une déontologie, voire d'engagements précis en la matière, qui feraient l'économie d'un règlement du dossier au fond ? Dans l'attente d'éléments, de fait précis lui permettant de répondre à ses inter-

rogations. Il lui demande de faire le point des derniers développements de ce dossier, en lui indiquant notamment l'état d'avancement des discussions concernant les activités du réseau Echelon avec les cinq pays concernés, au premier rang desquels le Royaume-Uni.

Réponse. — La croissance accélérée des réseaux mondiaux de télécommunication recèle des risques de dérapage préjudiciables aux droits des individus et à l'ordre public. Les lacunes dans le domaine de la sécurisation des informations empruntant les nouveaux réseaux ou accessibles depuis ces derniers multiplient les risques de piratage de données sensibles ou les atteintes à la vie privée. Ces actions peuvent être l'œuvre de particuliers comme des Etats. Il n'existe pas aujourd'hui de moyens d'empêcher, techniquement, l'interception des communications lorsqu'elles sont véhiculées dans un espace mondial qui ne connaît pas de frontières physiques. Les révélations sur les activités du réseau Echelon contenues dans un rapport du Parlement européen et largement reprises par les médias, n'ont pas fait l'objet, à ce jour, d'un traitement spécifique dans les discussions internationales. Si l'existence d'un tel réseau révèle effectivement, comme l'indique l'honorable parlementaire, l'absence d'une déontologie de la part des Etats qui utilisent les possibilités offertes par les nouveaux systèmes de communication à des fins préjudiciables, c'est précisément par la poursuite de discussions multilatérales que de telles règles pourraient émerger. En ce sens, le Gouvernement français poursuit une politique volontariste dans deux directions. La première se concrétise sous la forme d'une participation active dans les négociations internationales qui se sont ouvertes au sein de l'Union européenne, du conseil de I Europe ou du G 8. Comme l'a noté l'honorable parlementaire, ces travaux visent, d'une part, à améliorer les capacités des services répressifs et judiciaires en matière d'enquête et de poursuites de la criminalité liée à l'utilisation des technologies de pointe mais aussi à définir des limites à l'action des services nationaux au regard de la souveraineté de chaque Etat, de la protection des droits de l'homme, des libertés démocratiques et de la vie privée. Le second volet de cette politique vise à encourager, sur un plan national, le développement des moyens permettant de répondre aux besoins de confidentialité et d'intégrité des systèmes d'information sensibles. A cette fin, le cadre législatif français en matière de cryptologie et l'appel à projet OPIDUM (offre de produits de sécurisation pour la mise en œuvre des autoroutes de l'information) lancé au mois de septembre 1997 par le secrétariat d'état à l'industrie pour favoriser l'émergence de produits de sécurisation des échanges réalisés sur les réseaux constituent des éléments de réponse aux besoins identifiés. Des actions de sensibilisation, de protection contre les intrusions des systèmes de communication et de détection des menaces complètent le dispositif national qui se met en place. Enfin, le Gouvernement français indique à l'honorable parlementaire qu'il entend préserver ses propres capacités d'interception des communications telles que définies par la loi n° 91-646 du 10 juillet 1991 et nécessaires à la lutte contre les activités criminelles ou terroristes. A ce titre, l'autorisation récente d'exploiter un réseau de télécommunication par satellite accordée à Iridium, par arrêté du 28 octobre 1998, a été liée à la mise en place des moyens nécessaires à la mise en œuvre effective de la loi susmentionnée.

Assemblée nationale 22 février 1999 n° 8 (p. 1042)

SANTÉ

Statistiques et secret

19610 — 28 septembre 1998. — **M. André Gerin** attire l'attention de **M. le secrétaire d'Etat à la santé** sur le respect de la confidentialité des informa-

tions sur la santé de la population. Les progrès de la technologie ont permis ces dernières années d'aller très loin dans l'informatisation, la transmission rapide des données de quelque nature que ce soit. Les nouvelles procédures semblent très attractives du point de vue pratique et de la rationalisation des moyens. Concernant les renseignements sur la santé, les professionnels de la santé constatent dans leur quotidien des débuts de dérives de cette informatisation. Ils sont obligés de remplir des fiches nominatives par patient avec des informations de plus en plus détaillées portant sur leur état civil et sur les diagnostics établis. Ces fiches sont transmises au médecin responsable d'un département de l'information médicale (DIM) pour l'établissement de statistiques. Ces données nominatives sont centralisées hors du service traitant les patients. Il y a quelques années elles étaient centralisées dans le service et seules des données anonymes étaient fournies à des fins statistiques. Ce système pose de nombreuses questions. Même si les personnes concernées sont autorisées par la loi à traiter de telles informations, le secret professionnel du praticien est délégué à d'autres à l'insu des patients. De plus la notion de secret partagé n'existe pas dans notre droit. Ce système comporte de nombreuses failles permettant l'utilisation des données à des fins discriminatoires (captures ou vols informatiques, risques de fichier unique pour plusieurs utilisateurs…). Les difficultés sont encore plus aiguës pour les diagnostics psychologiques et psychiatriques qui sont de nature plus subjectifs. Cette remarque est également valable pour les services visant à la prévention. La mise en fiche est inadéquate et risque de catégoriser par exemple des enfants alors qu'il ne s'agit que d'incidents mineurs dans leur parcours psychologique. Il est impérieux de respecter la confidentialité entre les professionnels de la santé et les patients selon les principes des libertés individuelles et des droits de l'homme. Le technique sous aucun prétexte ne doit occulter ces principes fondateurs. Il lui demande quelle décision et quelles mesures entend prendre le Gouvernement pour réviser les textes et leur interprétation afin de revenir à un véritable anonymat des données informatiques sur la santé de la population.

Réponse. — Les données relatives au programme de médicalisation des systèmes d'information (PMSI) sont réunies au sein de l'établissement par le médecin responsable de l'information médicale. L'institution de ce médecin résulte d'une disposition législative introduite dans le code de la santé publique par l'article 40 de la loi n° 93-21 du 27 janvier 1993. Les modalités de la communication des données médicales nominatives nécessaires à l'analyse de l'activité des établissements de soins ont été définies par décret en conseil d'État après consultation du Conseil national de l'ordre des médecins. Ces données sont centralisées et traitées au sein de l'établissement hors du service ayant pris en charge le patient. Toutefois, le patient doit avoir été averti de la transmission de ces données au médecin responsable de l'information médicale de l'établissement, en vue de leur traitement automatisé (art. R 7105-7 du code de la santé publique). Le traitement de ces données nominatives doit faire l'objet d'une demande d'avis ou d'une déclaration préalable de l'établissement auprès de la commission informatique et liberté de même que la transmission aux organismes habilités doit faire l'objet d'un arrêté du ministre chargé de la santé après avis de la commission des systèmes d'information des établissements de santé. Malgré les précautions que traduisent ces procédures, les risques évoqués, qui tiennent aujourd'hui à la puissance mais aussi à la vulnérabilité dans certaines hypothèses des systèmes informatiques, doivent être pris en considération. Les sécurités informatiques et les conditions de traitement et de transmission de ces données doivent faire l'objet d'un contrôle attentif La mise en place du réseau santé social permettra d'accroître la sécurité de ces transmissions. Dans le même temps, la transposition de la directive européenne relative à la protection des personnes physiques à l'égard

du traitement des données à caractère personnel, qui classe les informations de santé parmi les données sensibles, pourrait conduire à une révision des procédures actuelles et à de nouvelles exigences en ce qui concerne la protection des patients.

Assemblée nationale 15 février 1999 n° 7 (p. 971)

SOCIAL

Typologies

9891 — 30 juillet 1998. — **M. Guy Fischer** appelle l'attention de **M. le ministre de 1'intérieur** sur 1'inquiétude que suscite 1'avis favorable de la Commission nationale de l'informatique et des libertés (CNIL) concernant l'utilisation d'un progiciel, déjà en usage dans certains départements, destiné à rendre possible la constitution d'un fichier unique départemental par individu ou par famille. L'une des fonctions de ce logiciel permet de dresser une typologie des potentialités et des difficultés des bénéficiaires de l'aide sociale. La liste de questions utilisée à cette fin fait appel à des appréciations subjectives sur l'individu, et nombre de travailleurs sociaux s'élèvent contre le caractère figé d'une telle typologie, et redoutent l'usage qui pourrait en être fait. Si l'informatisation des données sociales peut apparaître comme une solution de bon sens et offrir une plus grande rapidité de traitement des dossiers il n'en demeure pas moins que le Gouvernement doit pouvoir garantir à chaque citoyen la confidentialité des éléments concernant sa santé et sa vie sociale. Ainsi, même si la CNIL a souhaité que ce questionnaire demeure facultatif, la notion même de typologie paraît une grave atteinte aux libertés individuelles en comportant le risque de voir se constituer un fichage des populations défavorisées. Il lui demande donc de lui faire connaître son point de vue sur le traitement informatisé des données sociales. Il souhaite en outre savoir si le Gouvernement entend prendre position dans le débat que ne va pas manquer de susciter la réouverture de ce dossier par la CNIL en septembre prochain. — **Question transmise à M. le secrétaire d'Etat à la santé et à l'action sociale.**

Réponse. — Le développement et la mise en place d'un progiciel visant au traitement informatisé de données sociales concernant les personnes bénéficiaires des prestations délivrées par les services de certains départements a suscité des interrogations chez certains travailleurs sociaux concernés et leurs représentants. La Commission nationale informatique et libertés saisie, dès 1995, de la mise en œuvre d'un tel traitement informatisé, a rendu plusieurs avis dont le dernier en date du 13 octobre 1998 précise les garanties nécessaires pour un parfait anonymat des données. Depuis l'origine, le ministère de l'emploi et de la solidarité et le Conseil supérieur du travail social, placé auprès de lui, ont suivi ces évolutions avec une grande vigilance, et plus spécifiquement dans le cadre des récentes orientations du Premier ministre relatives au développement de la société de l'information. En effet, si l'on ne peut contester les bénéfices d'une telle procédure de traitement des données dès lors qu'elle reste dans le cadre des finalités expressément définies, il convient de l'encadrer de manière à ce qu'elle ne porte pas atteinte au principe de respect de la vie privée et qu'elle ne permette pas la constitution d'un fichier des populations fragilisées. Le Conseil supérieur du travail social, pour sa part, dans le cadre des mandats qui ont été définis par la ministre de l'emploi et de la solidarité, notamment celui sur les nouvelles technologies de l'information et de la communication et celui sur la déontologie des travailleurs sociaux, sera amené, dès le début 1999, à ouvrir un débat et formuler des avis et propositions tant sur l'informatisation des données sociales

que, de façon plus large, sur la responsabilité des travailleurs sociaux au regard notamment des principes déontologiques des professions.

Sénat 28 janvier 1999 n° 4 (p. 307)

TRAVAIL

Surveillance des salariés

31590 — 21 juin 1999. — **M. Vincent Buroni** appelle l'attention de **Mme la ministre de l'emploi et de la solidarité** sur les dangers de la surveillance des salariés dans l'entreprise par l'intermédiaire des nouvelles technologies. En effet, en 1998, la Commission nationale de l'informatique et des libertés (CNIL) a estimé à 28 000 le nombre d'entreprises qui ont installé un système de surveillance de leurs salariés, contre 6 500 en 1990. L'arsenal technologique déployé est impressionnant et sophistiqué (informatique, télécommunication, vidéosurveillance). Il fragilise ainsi le droit de chaque employé à protéger sa vie privée en milieu professionnel. En dépit d'un certain nombre de textes législatifs encadrant et limitant de tels actes notamment la loi de janvier 1978 sur les fichiers nominatifs et la loi de décembre 1991 sur la transparence dans l'entreprise, ces dispositifs ne sont que partiellement appliqués sur le terrain. A ce titre, il lui demande quelles mesures elle entend adopter pour limiter à une stricte légalité l'exercice de telles pratiques.

Réponse. — L'attention de Mme la ministre de l'emploi et de la solidarité a appelée sur le fait que de plus en plus d'entreprise développent une surveillance de leurs salariés sur les lieux de travail, en s'appuyant sur le progrès des technologies fondées, notamment sur la vidéo. Il lui est demandé quelles dispositions le Gouvernement entend prendre pour éviter que de telles mesures ne menacent le droit des salariés à leur vie privée sur le lieu de travail Ainsi que le mentionne l'honorable parlementaire, il existe d'abord des dispositions spécifiques permettant de protéger les salariés de tels abus introduites par les lois sur l'informatique et les libertés de 1978 et par la loi de 1991 sur la transparence des entreprises. Le code du travail comporte également une série de dispositions protégeant les salariés contre de semblables abus. Ainsi, l'article L 120-2 du code du travail (issu de la loi n. 92-144 du 31 décembre 1992) dispose que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature des tâches à accomplir ni proportionnées au but recherché. » De même, l'article L. 122-35 du code du travail prévoit que : « Le règlement intérieur ne peut contenir de clause contraire aux lois et règlements, ainsi qu'aux dispositions des conventions et accords collectifs de travail applicables dans l'entreprise et l'établissement ». Le chef d'établissement est donc tenu de respecter la liberté individuelle des salariés et ne peut, par aucune mesure, mettre en cause leurs droits fondamentaux sur le lieu de travail. En toute état de cause si, en dépit de ce corps de règles, des entreprises mettent en place des dispositifs visant à surveiller de manière abusive les salariés à des fins étrangères à de légitimes motifs de sécurité, ces derniers peuvent saisir leurs représentants. En application de l'article L. 422-1-1 du code du travail, « si un délégué du personnel constate, notamment par l'intermédiaire d'un salarié, qu'il existe une atteinte aux droits des personnes ou aux libertés individuelles dans l'entreprise qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché, il en saisit immédiatement l'employeur. L'employeur ou son représentant est tenu de procéder sans délai à une enquête avec le délégué et de prendre les dispositions nécessaires pour remédier à cette situation. En cas de carence de l'employeur..., le salarié ou le délégué... saisit le bureau de jugement du conseil des Prud'hommes... ». En outre, avant de recourir au juge les salariés ou leurs

représentants peuvent en toute confidentialité, demander à l'inspection du travail de s'opposer à des mesures manifestement illégales. Il est également important de rappeler que l'article L. 432-2-1 du code du travail prévoit que le comité d'entreprise est obligatoirement informé, préalablement à leur introduction dans l'entreprise, sur… « les traitements automatisés de gestion du personnel » sur toute modification de ceux-ci. Le même article du code du travail prévoit ensuite une disposition, qui constitue une garantie importante de protection des salariés contre les pratiques que vous évoquez. Il dispose en effet » que le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise… sur les moyens ou les techniques permettant un contrôle de l'activité des salariés « . Compte tenu du régime de protection existant, il n'apparaît donc pas indispensable de prendre l'initiative de mesures complémentaires pour combattre efficacement les dérives redoutées.

Assemblée nationale 18 octobre 1999 n° 42 (p. 6054)

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 À 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.

La protection des données en Europe et dans le Monde

1 — Dans l'Union européenne

Pays	Convention 108	Législation	Autorité de contrôle
Allemagne	ratification : 18/06/85 entrée 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. ◆ Transposition directive 95/46/CE : Projet de loi	Der Bundesbeauftragte für den Datenschutz (autorité fédérale) Postfach 200112 - 53131 Bonn Web : www.datenschutz.de
Autriche	ratification : 30/03/88 entrée en vigueur : 01/07/88	◆ Loi fédérale sur la protection des données du 18 octobre 1978, amendée en 1986. ◆ Transposition directive 95/46/CE : Loi dite "loi 2000". (en vigueur au 1 er janvier 2000)	Direktor Buro der Datenschutzkommission und des Datenschutzrates Bundeskanzleramt Ballhausplatz 1- 1014 Vienne
Belgique	ratification : 28/05/93 entrée 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.	Commission de la protection de la vie privée Porte de Hal, 5-8 Bruxelles 1060 Web : www.privacy.gov.be
Danemark	ratification : 23/10/89 entrée 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 2e projet de loi en attente au parlement depuis oct 99.	Registertilsynet Christians Brygge 28 4 sal 1559 Copenhague Web : www.registertilsynet.dk
Espagne	ratification : 31/01/84 entrée 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 Po de la Castellana 41, 5.a planta, Madrid 28046 Web : www.ag-protecciondatos.es
Finlande	ratification : 02/12/91 entrée 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 du 10 février 1999. (en vigueur depuis le 1er juin 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
France	ratification : 24/03/83 entrée 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 : Projet de loi.	Commission Nationale Informatique et Libertés 21, rue Saint-Guillaume 75740 Paris cedex 07 Web : www.cnil.fr
Grèce	ratification : 11/06/95 entrée 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	ratification : 25/04/90 entrée 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
Italie	ratification : 29/03/97 entrée 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.	Garante per la protezione dei dati personali Largo del Teatro Valle 6 00186 Rome
Luxembourg	ratification : 10/02/88 entrée 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	ratification : 24/08/93 entrée 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 : Projet de loi.	Registratiekamer Prins Clauslaan 20 Postbus 93374 - 2509 AJ's-Gravenhage Web : www.registertiekamer.nl
Portugal	ratification : 02/09/93 entrée 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
Royaume-uni	ratification : 26/08/87 entrée 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.	Data Protection Registrar Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF United Kingdom Web : www.dataprotection.gov.uk
Suède	ratification : 29/09/82 entrée en vigueur : 01/10/85	◆ Loi du 11 mai 1973 sur la protection des données. ◆ Transposition directive 95/46/CE : Loi du 24 octobre 1998 sur la protection des données.	Datainspektionen Box 8114 104 20 Stockholm Web : www.datainspektionen.se

2 — Hors de l'Union européenne

Pays	Convention 108	Législation	Autorité de contrôle
Argentine		◆ Loi sur la protection des données personnelles -1996 (non promulguée à ce jour)	
Australie		◆ Loi fédérale sur la vie privée -1988 (Secteur public)	Human rights and equal opportunity 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	Federal privacy commission Tower B, 3rd Floor, 112 Kent Street - Otawa, Ontario K1A 1H3 Web: www.privcom.gc.ca
Corée (sud)		◆ Loi sur la protection des données personnelles -1994	
Estonie	signature : 24/01/00	◆ Loi sur la protection des données personnelles -1996	
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)	
Guernsey		◆ Loi sur la protection des données - 1986	The data protection officer PO Box 43 La Charroterie St Peter Port G71 1FH
Hong-Kong		◆ Loi sur la protection des données - 1990 ◆ Ordonnance sur la protectiondes données - 1995	Privacy commission for personal data Unit 2001, 20/F - OfficeTower Convention Plaza - 1 Harbour Road Wan Chai - Hong Kong Web: www.pco.org.hk
Hongrie	ratification : 08/10/97 entrée 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 Tüköry u 3 H-1054 Budapest
Ile de man		◆ Loi sur la protection des données - 1986	Data protection registrar PO Box 69 Douglas IM99 1EQ - Ile de Man
Islande	ratification : 25/03/91 entrée en vigueur : 01/07/91	◆ Loi n° 63-1981 relative l'enregistrement de données personnelles -1981 (amendée en 1989)	Icelandic Data Protection Commission Arniarhvoll 150 Reykjavik
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 Ministry of justice Hillel Street 6 PO Box 2808 Jerusalem 91027

Pays	Convention 108	Législation	Autorité de contrôle
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		◆ Loi sur la protection des données - 1987	Data protection registry States Greffe Westway Chambers Don Street St Helier JE 24TR
Lettonie		◆ Loi sur la protection des données - 1998	
Lituanie		◆ Loi sur la protection des données personnelles - 1996	
Moldavie	signature : 04/05/98		
Monaco		◆ Loi n°1.165 relative aux traitements d'informations nominatives 1993	Commission de contrôle des informations nominatives Ministère d'Etat Place de la visitation 98000 Monaco
Norvège	ratification : 20/02/84 entrée en vigueur : 1/10/85	◆ Loi sur les registres de données personnelles - 1978	Datatilsynet 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 - 1993	Privacy commission PO Box 466 Auckland Web: www.privacy.org.nz
Pologne	signature : 21/04/99	◆ Loi sur la protection des données personnelles - 1997	
Rép. de St-Marin		◆ Loi relative à la protection des données personnelles - 1983 (amendée en 1995)	
Rép. Tchèque		◆ Loi relative à la protection des données personnelles des systèmes informatisés - 1992	
Roumanie		◆ 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 informations 1995	
Slovaquie	signature : 14/04/00	◆ Loi relative à la protection des données personnelles des systèmes informatisés 1998	
Slovénie	ratification : 23/11/93 entrée en vigueur : 01/09/94	◆ Loi n° 210-01/89-3 sur la protection des données - 1990	

Pays	Convention 108	Législation	Autorité de contrôle
Suisse	ratification : 02/10/97 entrée 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	Official Information Commission's Office The prime Minister's Office Governement House Bangkok 10300 Thailand

Travaux du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (art. 29)

5093/98/FR/FINAL WP 17

RECOMMANDATION 1/99 SUR LE TRAITEMENT INVISIBLE ET AUTOMATIQUE DES DONNÉES À CARACTÈRE PERSONNEL SUR L'INTERNET EFFECTUÉ PAR DES MOYENS LOGICIELS ET MATÉRIELS
Adoptée par le Groupe le 23 février 1999

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, vu l'article 29 et l'article 30, paragraphe 3, de ladite directive, vu son règlement intérieur, notamment ses articles 12 et 14,

A adopté la présente recommandation :

1 — Le Groupe encourage l'industrie du logiciel et du matériel informatique à travailler sur des produits respectant la vie privée sur l'Internet qui fournissent les outils nécessaires pour se conformer aux règles européennes relatives à la protection des données.

Pour que le traitement des données à caractère personnel soit légitime, il faut que la personne concernée soit informée d'un tel traitement et qu'elle en ait donc connaissance. Par conséquent, le Groupe est particulièrement préoccupé par toutes sortes d'opérations de traitement qui sont actuellement effectuées sur l'Internet par des moyens logiciels et matériels à l'insu de la personne concernée, pour laquelle elles sont donc « invisibles ».

Parmi les exemples types d'un tel traitement invisible figurent le « chattering » au niveau HTTP [1], les hyperliens automatiques vers des tiers, le contenu actif (comme Java, ActiveX ou autres technologies exécutant des scripts dans le client) et le mécanisme des cookies tel qu'il est actuellement mis en œuvre dans les logiciels de navigation courants.

2 — Les logiciels et matériels informatiques pour l'Internet devraient informer les internautes sur les données destinées à être recueillies, stockées ou transmises et leur indiquer à quelles fins ces données sont nécessaires.

Ces logiciels et matériels informatiques devraient également permettre à tout moment un accès aisé de l'utilisateur aux données recueillies à son sujet.

Cela signifierait par exemple que :
— dans le cas d'un logiciel de navigation, lorsqu'il établit une connexion avec un serveur Web (envoi d'une requête ou réception d'une page Web), l'utilisateur serait informé des informations destinées à être transmises et à quelles fins ;
— en cas d'envoi, par un moyen quelconque, d'hyperliens par un site Web à un utilisateur, le logiciel de navigation de l'utilisateur devrait tous les lui indiquer ;

1 En pareil cas, les informations transmises dans la requête http contiennent plus de données qu'il n'est nécessaire pour contacter le serveur.

— dans le cas des cookies, l'utilisateur devrait être averti avant leur réception, leur stockage ou leur transmission par le logiciel Internet. Le message devrait préciser, dans un langage généralement compréhensible, quelles informations vont être stockées dans le cookie et à quelles fins, ainsi que la période de validité de celui-ci.

3 — La configuration par défaut des matériels informatiques et des logiciels devrait ne pas permettre la collecte, le stockage ou l'envoi d'informations permanentes sur le client [1]. Par exemple :
— le logiciel de navigation devrait être configuré par défaut de telle sorte que seule soit traitée la quantité minimale d'informations nécessaire à l'établissement d'une connexion Internet. Les cookies devraient, par défaut, ne pas être envoyés ou stockés ;
— lors de son installation, la partie d'un logiciel de navigation destinée à stocker et à envoyer des données concernant l'identité de l'utilisateur ou son comportement de communication (profil) ne devrait pas être remplie automatiquement avec des données stockées précédemment dans le matériel de l'utilisateur.

4 — Les matériels informatiques et les logiciels pour l'Internet devraient permettre à la personne concernée de décider librement du traitement de ses données personnelles en lui proposant des outils conviviaux pour filtrer (c'est-à-dire pour refuser ou modifier) la réception, le stockage ou l'envoi d'informations permanentes sur le client selon certains critères (notamment les profils, le domaine ou l'identité du serveur Internet, le type et la durée des informations recueillies, stockées ou envoyées, etc.). L'utilisateur devrait obtenir des instructions claires concernant l'usage des logiciels et matériels informatiques pour la mise en œuvre de ces options et outils. Par exemple :
— le logiciel de navigation devrait comporter des options permettant à l'utilisateur de le configurer en précisant quelles informations celui-ci devrait ou ne devrait pas recueillir et transmettre ;
— en ce qui concerne les cookies, l'utilisateur devrait toujours avoir la possibilité d'accepter ou de refuser l'envoi ou le stockage d'un cookie dans son ensemble. En outre, l'utilisateur devrait avoir le choix de déterminer quelles données devraient être conservées dans un cookie ou supprimées, en fonction, par exemple, de la durée de validité de celui-ci ou des sites Web qui l'envoient et le reçoivent.

5 — Les logiciels et matériels informatiques pour l'Internet devraient permettre aux utilisateurs de supprimer les informations permanentes sur le client d'une manière simple et sans faire intervenir l'expéditeur. L'utilisateur devrait obtenir des instructions claires sur la façon de procéder. Si ces informations ne peuvent pas être supprimées, il faut prévoir un moyen fiable d'empêcher leur transfert et leur lecture.

— Les cookies et autres informations permanentes sur le client devraient être stockés d'une façon standardisée et devraient pouvoir s'effacer facilement et sélectivement dans l'ordinateur du client.

Contexte

À l'heure actuelle, il est presque impossible d'utiliser l'Internet sans être en présence d'éléments constituant une intrusion dans la vie privée, qui traitent toutes

1 Les information permanentes sur le client, expression technique (et non juridique), désignent des données relatives au client (le PC de l'utilisateur) qui subsistent pendant plus d'une session dans le matériel informatique. Une session commence lorsque le client appelle une page sur un site Web donné et se termine au moment où il décide de fermer le logiciel de navigation ou d'éteindre l'ordinateur ou lorsqu'il appelle une page d'un autre site Web. Les cookies sont un exemple type d'informations permanentes sur le client, de même que les préférences en matière de vie privée.

sortes de données à caractère personnel d'une manière qui est invisible pour la personne concernée. En d'autres termes, l'internaute ignore que des données à caractère personnel le concernant ont été recueillies et retraitées et que celles-ci pourraient servir à des fins qui lui sont inconnues. La personne concernée n'a pas connaissance de ce traitement et n'a aucune liberté de choix à l'égard de celui-ci.

Un exemple de ce type de procédé est ce qu'on appelle le cookie, qui peut se définir comme un relevé informatique de données qui est envoyé d'un serveur Web vers l'ordinateur d'un utilisateur en vue de l'identification future de cet ordinateur lors des visites ultérieures sur ce même site Web.

Les navigateurs sont des logiciels qui servent notamment à afficher graphiquement les documents présents sur l'Internet. Ils instaurent une communication entre l'ordinateur de l'utilisateur (le client) et le serveur où les informations sont stockées (le serveur Web). Ces logiciels de navigation transmettent souvent plus de données au serveur Web que ce qui est strictement nécessaire pour établir la communication. Les navigateurs classiques transmettront automatiquement au serveur Web visité le type et la langue du navigateur, le nom d'autres logiciels installés sur le PC de l'utilisateur et du système d'exploitation, la page contenant le renvoi, les cookies, etc. Ces données peuvent aussi être transmises systématiquement à des tiers par le logiciel de navigation, et ce de manière invisible.

Ces techniques permettent de créer des « clicktrails » sur l'internaute. Il s'agit d'informations sur son comportement, son identité, le chemin emprunté ou les choix exprimés lors de la visite d'un site Web. Ces « clicktrails » contiennent les liens qu'un utilisateur a activés et sont enregistrés dans le serveur Web.

Les directives européennes 95/46/CE et 97/66/CE sur la protection des données contiennent des dispositions détaillées relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ces deux directives sont applicables aux situations examinées dans la présente recommandation car les données à caractère personnel concernant les internautes sont traitées dans ce contexte. Les cookies ou les logiciels de navigation peuvent contenir ou retraiter des données permettant l'identification directe ou indirecte de l'internaute individuel.

L'application des dispositions sur le traitement loyal, les raisons légitimes du traitement et le droit de la personne concernée de décider du traitement de ses propres données ont donné lieu à la recommandation ci-dessus.

Le groupe de travail est particulièrement préoccupé par les risques inhérents au traitement des données à caractère personnel concernant des personnes qui ignorent totalement l'existence d'un tel traitement. Les concepteurs de logiciels et de matériel informatique sont donc incités à prendre en considération et respecter les principes de ces directives afin de mieux protéger la vie privée des internautes.

5026/99/FR/FINAL WP 20

AVIS 3/99 CONCERNANT L'INFORMATION ÉMANANT DU SECTEUR PUBLIC ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL CONTRIBUTION À LA CONSULTATION INITIÉE PAR LIVRE VERT DE LA COMMISSION EUROPÉENNE INTITULÉ « L'INFORMATION ÉMANANT DU SECTEUR PUBLIC : UNE RESSOURCE CLEF POUR L'EUROPE COM (1998) 585

Adopté le 3 mai 1999

Introduction et observations préliminaires :

1 — La Commission européenne a soumis à consultation publique un livre vert sur « l'information émanant du secteur public : une ressource clé pour l'Europe » [1].L'objet principal du livre vert consiste à promouvoir une discussion sur la question de savoir comment rendre l'information détenue par le secteur public plus accessible aux citoyens et entreprises ainsi que sur la nécessité ou non d'harmoniser les règles nationales dans ce domaine. Ce document paraît assez largement inspiré par la revendication des acteurs privés qui souhaitent avoir un accès au moindre coût aux informations publiques et contestent le maintien de monopoles publics dans ce domaine.

Un des enjeux du livre vert concerne donc la mise à disposition de l'information émanant du secteur public, c'est à dire d'une catégorie particulière de données dites « publiques » : celles qui, détenues par des organismes du secteur public, seraient rendues publiques en vertu de règles ou d'un usage [2] dont le fondement implicite ou explicite peut être trouvé dans une volonté de transparence de l'état à l'égard de ses citoyens [3].

La protection des données à caractère personnel n'est pas ignorée par ce document, même si elle n'apparaît pas en constituer l'enjeu majeur.

Le point 111 (II. 7, page 17) mentionne explicitement que la directive 95/46/CE sur la protection de données à caractère personnel [4] « établit des règles obligatoires pour les secteur publics et privés et [...] est pleinement d'application dans le cas où des données à caractère personnel sont détenues par le secteur public ».

Le point 114 souligne que « l'émergence de la société de l'information pourrait poser de nouveaux risques pour la vie privée des individus si des registres publics venaient à être accessibles sous forme électronique (en particulier en ligne et sur Internet et dans de larges quantités) ».

Pourtant, le livre vert dans son ensemble fait naître plusieurs ambiguïtés sur la force de cette conviction.

1 Com 1998 585, disponible à l'adresse suivante : http://www.echo.lu/legal/en/access.htlm.
2 Il semble qu'une distinction puisse être faite entre la publicité ordonnée par une législation, l'accèss à l'information autorisé par la loi et des situations dans lesquelles la question de la publicité ou de l'accès se pose suite à une demande formulée par des particuliers ou des entreprises à l'égard du secteur public sans qu'une loi la réglemente.
3 Le présent avis ne traite donc pas de l'autre acception — la plus large — du terme de donnée dite « publique » : celle qui couvre l'ensemble des données traitées par des autorités publiques.
4 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, JO L 281, 23 novembre 1995, p. 31. Disponible à l'adresse suivante : http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.h tm.

En premier lieu, l'utilisation (dans la version anglaise) du terme « publicly available » (publiquement disponible) est propice à la conception selon laquelle des données rendues publiques seraient, de ce fait, disponibles pour tout usage. On relèvera que le principe de finalité, pilier de nos législations de protection des données, s'accommode mal de l'adjectif « disponible ». En outre, le principe de la loyauté de la collecte — garanti notamment par l'exigence de sécurité des traitements — pourrait souffrir qu'une donnée soit rendue publique sans réflexions ni précautions. Aussi conviendrait-il que l'expression « publicly available » soit écartée au profit d'une autre expression plus appropriée et sans ambiguïté (par exemple « publicly accessible »)

En deuxième lieu, la question n 7 (« les considérations liées au respect de la vie privée méritent-elles une attention particulière au regard de l'exploitation de l'information émanant du secteur public ? », page 17) pourrait donner à penser que le rappel des dispositions de la directive 95/46/CE ne conduit pas aussi fermement qu'on aurait pu l'imaginer à des conclusions précises sur ce point, alors même qu'il est précisé (point 111) que la directive 95/46/CE « réalise l'équilibre nécessaire entre le principe de l'accès à l'information du secteur public et la protection des données à caractère personnel ». Ces ambiguïtés doivent être levées.

2 — Dans ce contexte, le présent avis a pour objectif de nourrir la réflexion sur la dimension de la protection des données à caractère personnel qui est essentielle lorsque l'on s'engage à faciliter l'accès aux données du secteur public dès lors que celles ci portent sur des personnes physiques. Il ne prétend cependant pas fournir toutes les réponses aux questions que soulève dans tous les cas la conciliation entre l'objectif de faciliter l'accès aux données du secteur public fondée sur la volonté de renforcer la transparence des Etats à l'égard des citoyens et la protection des données à caractère personnel telle que définie par la directive européenne 95/46/EC.

Ainsi, cet avis ne traitera pas des questions soulevées par le livre vert qui semblent dépasser la seule mise à disposition de tiers de l'information émanant du secteur public, comme par exemple le point de vue exprimé au point 56 (II ; 2, page 10) que « l'utilisation des nouvelles technologies peut de façon importante accroître l'efficacité de la collecte d'information. Elle offre aux organismes publics la possibilité de partager l'information disponible, lorsque cela est conforme aux règles de protection des données ».

Son but est de fournir, sur la base de la directive 95/46/CE ainsi que d'expériences concrètes prises à des fins pédagogiques dans le champ de registres les plus connus de données à caractère personnel rendues publiques, un premier ensemble de points de repère qu'il convient de prendre en considération lorsque des décisions concrètes sont prises. Ces points de repère et exemples concrets pris dans divers Etats membres, sont destinés à illustrer comment dans la société de l'information, doivent être prises en compte les règles de protection des données à l'égard des données issues de registres publics et, certaines des mesures d'ordre technique ou organisationnel qui peuvent contribuer (sans toutefois prétendre à garantir une protection sans faille) à concilier la publicité de ces données et le respect des dispositions de protection des données à caractère personnel et en particulier celles relatives au principe fondamental en la matière à savoir le principe de finalité pour laquelle les données sont, dans le cas qui nous intéresse ici, rendues publiques.

I — Les règles de protection des données s'appliquent aux données à caractère personnel rendues publiques

L'accessibilité des informations relevant du secteur public, notamment par voie d'informatisation, préconisée par le livre vert, pose la question de savoir de quelles façons ces informations sont utilisées. Leur utilisation ne saurait être interdite,

tel n'est pas le sens de l'évolution de nos sociétés. Tel n'est pas, non plus, le sens de nos législations de protection des données, garantes de l'accompagnement de l'informatisation de la société et non de sa prohibition.

Au demeurant, affirmer l'applicabilité de nos lois de protection des données aux données personnelles rendues publiques, n'est que l'expression d'une évidence résultant des textes sur la protection des données : une donnée à caractère personnel, même rendue publique, reste une donnée à caractère personnel et bénéficie, dès lors, d'une protection.

Cette affirmation implique nécessairement de déterminer la protection qui est offerte à la donnée à caractère personnel rendue publique. A cet égard, le directive 95/46/CE apporte d'ores et déjà des réponses.

A — La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

La directive permet de prendre en compte dans la mise en œuvre des règles qu'elle pose, le principe du droit d'accès du public aux documents administratifs [1] ainsi que d'autres éléments pertinents pour la discussion [2].

Ainsi le principe de finalité exige que des données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ses finalités. [3] Ce principe joue donc un rôle central dans la mise en œuvre de l'accessibilité de données à caractère personnel détenues par le secteur public.

Il convient notamment de déterminer au cas par cas dans quelle mesure une loi exige ou autorise la publication ou l'accès par le public à des donnés à caractère personnel : vise-t-elle une accessibilité intégrale et illimitée dans le temps, permet-elle une utilisation de ces données à n'importe quelle fin indépendamment de la finalité initiale ou, bien au contraire, est-ce que la loi prévoit une accessibilité seulement pour certaines parties et/ou une utilisation liée à la finalité pour laquelle la donnée a été rendue publique ? Par conséquent, il n'existe pas une seule catégorie de données à caractère personnel destinée à être rendue publique qui devrait être traitée uniformément du point de vue de la protection des données, mais il convient plutôt de procéder dans l'analyse par degrés dans la délimitation des droits de l'individu concerné par les données et des droits du public à accéder à l'information respectivement. Bien que l'accès aux données puisse être public, il peut être soumis à des conditions (tel que justification d'un intérêt légitime) ou encore l'exploitation de celles-ci, par exemple à des fins commerciales ou par les médias, peut être restreinte. Les exemples infra vont illustrer ces questions.

Il est utile de rappeler ici qu'indépendamment d'une publication ou non de données à caractère personnel, la personne concernée a toujours le droit d'accès à ses données et le droit d'exiger, le cas échéant, leurs rectification ou l'effacement de données dont le traitement n'est pas conforme à la directive notamment en raison de leur caractère incomplet ou inexact [4].

1 Voir le considérant 72. Il convient de noter pour la discussion que la directive ne contient pas de définition du terme « documents administratifs », mais qu'il peut être entendu dans un sens large permettant de couvrir au moins les « informations administratives » envisagées par le livre vert dans sa proposition de classification des informations (point 73 et suivant, page 12).
2 Voir l'article 10 et considérant 37 de la directive 95/46/CE sur la conciliation du droit à la vie privé avec les règles régissant la liberté d'expression. Voir également la Recommendation 1/97 du Groupe sur « Législation sur la protection des données et médias », adopté le 25.2 1997 (document 5012/9, disponible dans les 11 langues à l'adresse indiquée en note de bas de page 1).
3 Voir en détail l'article 6 paragraphe 1 lettre b) de la directive 95/46/EC.
4 Voir article 12 de la directive 95/46/EC.

Certes, diverses dispositions de la directive font explicitement référence au caractère public d'une donnée. Deux de ces dispositions méritent d'être cités dans toutes leurs nuances.

L'article 18.3 qui impose que les traitements soient notifiés à l'autorité de contrôle permet de faire exception à cette obligation pour les registres « qui, en vertu de dispositions législatives ou réglementaires (…*sont*) destiné (s) à l'information du public et ouverts à la consultation du public « . Mais on relèvera que les considérants 50 et 51 de la directive précisent que ces exonérations ou simplifications ne s'appliquent qu'aux traitements dont le seul but (1re condition) est de tenir un registre destiné, dans le respect du droit national, à l'information du public (2e condition) et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime (3e condition), le bénéfice de telles dérogations ne dispensant le responsable du traitement d'aucune des autres obligations découlant de la directive.

Enfin, l'article 26.1.*f* qui déroge à l'exigence d'un niveau adéquat de protection pour les données faisant l'objet d'un flux vers des pays tiers lorsque le transfert des données à destination d'un pays n'offrant pas ce niveau de garantie est réalisé « au départ d'un registre tenu à la disposition du public ». Cependant, le considérant 58 de la directive limite la portée du transfert en précisant qu'il ne doit pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre et que, le cas échéant, le transfert ne doit pouvoir être effectué qu'à la demande des personnes qui y ont un intérêt légitime.

Mais il résulte clairement de ces dispositions et de ces précisions que si la protection des données à caractère personnel ne doit pas faire obstacle au droit des citoyens d'avoir accès aux documents administratifs dans les conditions prévues par chaque législation nationale, la directive n'a pas entendu pour autant priver les données accessibles au public de toute protection.

La discussion portant sur la question de savoir s'il y a un besoin d'harmoniser les règles nationales sur l'accès à l'information émanant du secteur public doit en tout état de cause tenir compte des règles harmonisées sur la protection des données à caractère personnel, ainsi que des mesures nationales les transposant.

Outre la mission de la Commission de veiller à l'application de la directive, il appartiendra au Groupe établit par l'article 29 de la directive d'apprécier concrètement la portée des dispositions nationales prises en application de la directive 95/46/CE dans les cas précis qui pourrait faire apparaître des divergences au plan national. [1]

B — Exemples de conciliation des règles de la protection des données à caractère personnel et de l'accès aux informations émanant du secteur public

Certaines législations subordonnent la diffusion d'informations détenues par le secteur public à certaines finalités qui peuvent interdire l'accès à certaines données, interdire certains usages des données ou poser des conditions à leur accès.

Or, la numérisation des informations et les possibilités de recherche en texte intégral peuventmultiplier à l'infini les possibilités d'interrogation et de tri, la diffusion par Internet accroissant les risques de captation et de détournement d'usage. De plus le rapprochement de données rendues publiques à partir de sources différentes est, lorsque celles-ci sont mises à la disposition du public, grandement facilité par la numérisation des données et permet notamment d'établir des profils sur la situation

1 Voir les articles 29 et 30 de la directive 95/46/EC.

ou le comportement d'individus [1]. En outre, il convient d'accorder une attention particulière au fait qu'en mettant ainsi des données à caractère personnel à la disposition du public, on alimente dans une large mesure les nouvelles techniques du « data warehousing » et du « data mining ». Ces procédés permettent de collecter des données sans aucune spécification à priori de la finalité, et ce n'est qu'au stade de l'exploitation que les diverses finalités sont définies. Dès lors, il faut tenir compte du fait de tout ce qui est techniquement possible de faire avec les données [2].

C'est pourquoi il convient de vérifier, au cas par cas, quelles pourraient être les répercussions négatives sur l'individu avant toute décision de diffusion sur support numérique. Selon le cas, il convient soit de décider de ne pas diffuser certaines données à caractère personnel, soit d'en soumettre la diffusion à l'appréciation de la personne concernée ou à d'autres conditions.

1 — Les bases de données issues des décisions de justice :

Le point 74 du livre vert (page 11) qui fait notamment référence aux jugements des tribunaux, pour illustrer le concept d'information fondamentale au fonctionnement de la démocratie « , soulève une interrogation de fond. En effet, peut-on concevoir que tous les jugements de toutes les juridictions soient disponibles sur Internet sans porter préjudice aux personnes.

Instruments de documentation juridique, les bases de données jurisprudentielles peuvent devenir, sans précautions particulières, des fichiers de renseignements sur les personnes si on les consulte non pour connaître une jurisprudence mais pour obtenir par exemple toutes les décisions de justice se rapportant à un même personne.

La Commission de la Protection de la Vie Privée (Belgique), dans un avis du 23 décembre 1997, l'a souligné avec force : « l'évolution technologique doit s'accompagner d'une plus grande retenue lors de la mention de l'identification des parties dans les chroniques de jurisprudence ». Elle propose qu'à défaut d'une anonymisation complète, les décisions de justice accessibles à tout public ne soient pas indexées à partir du nom des parties afin d'interdire les recherches à partir de ce critère.

La Commission de protection des données personnelles italienne [3] envisage de proposer au plan national que les parties disposent d'un droit d'opposition à la publication de leur nom dans les bases de données jurisprudentielles. Ce droit pourrait s'exercer à tout moment et être pris en compte lors des mises à jours des bases de données diffusées sur support magnétique. L'exercice de ce droit serait sans effet rétroactif pour les publications sur support papier.

En France, le ministère de la justice, qui souhaite diffuser les bases de données jurisprudentielles sur Internet, a imposé, dans le cahier des charges, l'anonymisation des décisions de justice.

2 — Certains textes officiels :

La diffusion d'informations sur Internet implique une profusion d'informations à l'échelle du monde et une multiplication de leurs sources. Ce changement d'échelle géographique peut faire naître un risque particulier. En effet, la diffusion d'une information légitimement publique dans un pays est, à l'échelle mondiale, sus-

1 A noter que l'utilisation de telles technologies donne également à l'état la possibilité d'établir de tels profiles.
2 Autre exemple : grâce au recoupement électronique de deux banques données, on peut obtenir plus facilement des informations négatives sur telle ou telle personne, par exemple : le recoupement du registre de population (lorsqu'il existe) et des listes électorales permet d'identifier les personnes n'ayant pas le droit de vote.
3 Garante per la protezione dei dati personali

ceptible de provoquer des atteintes graves à la vie privée ou à l'intégrité physique des personnes. Il en est ainsi, lorsque, par exemple, les décisions de naturalisation font l'objet d'une publication officielle de manière obligatoire Tel est le cas en France où, suivant en cela l'avis de la Commission Nationale de l'Informatique et des Libertés (CNIL), le Gouvernement français, lors du basculement sur Internet du Journal Officiel, a exclu ces textes d'une telle diffusion dans le souci d'éviter à certains ressortissants ayant abandonné leur nationalité d'origine le risque d'encourir d'éventuelles représailles.

Ainsi, dans certains cas, la volonté de transparence d'un Etat, et en particulier de ses ressortissants, peut mal s'accommoder de la diffusion planétaire de telles informations.

3 — Autres exemples de diffusion de données à caractère personnel rendues publiques soumises à des conditions de nature à protéger la personne concernée :

Les conditions d'accès aux données à caractère personnel contenues dans des registres peuvent être très variées, selon les réglementations : par exemple, accès partiel aux données du registre, preuve d'un intérêt, interdiction de l'usage commercial.

Ainsi, en Allemagne toute liste de candidats à une élection fédérale doit comporter leur nom, prénom, profession ou situation, jour, lieu de naissance et adresse. Cependant, sur les listes rendues publiques avant le scrutin par le responsable local ou du Land chargé de l'organisation des élections fédérales le jour de naissance est remplacé par l'année de naissance.

En Italie, la législation relative au registre de la population, tenu par chaque municipalité, prévoit l'interdiction de la communication des données à un organisme privé et l'obligation de toute administration qui demanderait la communication des données d'apporter la preuve d'un intérêt public pertinent.

En France, la liste électorale est publique aux fins du contrôle de sa régularité. La loi en permet l'utilisation à des fins politiques par tous les candidats et tous les partis et en interdit l'usage commercial. Il ne serait pas imaginable, en l'état, que les listes électorales puissent être diffusées sur Internet.

De même, en France, les données à caractère personnel contenues dans le cadastre sont publiques, mais il est interdit d'en faire un usage commercial.

En Grèce, le présent système du cadastre organisé sur base d'un registre alphabétique des propriétaires de biens immobiliers sera remplacé par un registre basé sur l'identification du bien immobilier afin d'empêcher que les recherches portent sur l'ensembles des biens immobilier appartenant à une même personne. L 'accès au cadastre est soumis à la justification d'un intérêt légitime.

II — Les nouvelles technologies peuvent contribuer à concilier la protection des données personnelles et leur publicité

Les nouvelles technologies, et certaines mesures administratives d'accompagnement, sont de nature, tout en favorisant l'accès aux données publiques, notamment par leur « mise en ligne », à faciliter le respect des principes majeurs de la protection des données tels que le principe de finalité, celui de l'information et du droit d'opposition ou celui de la sécurité. Toutefois, l'utilisation de ces technologies ne présente pas une garantie absolue contre le risque d'abus et de détournement de principes de protection des données à caractère personnel tels que décrit supra.

A — Les conditions techniques d'accès aux informations émanant du secteur public doivent contribuer au respect du principe de finalité

Compte tenu des conditions d'accessibilité numérique du public, il est certainement très difficile de garantir dans la pratique la spécification de la finalité, mais un recours réfléchi et ciblé à la technique doit contribuer à atteindre cet objectif. Il convient pour cela de vérifier et de définir dans chaque cas les conditions d'interrogation. À cet égard, le principe suivant devrait s'appliquer : « chacun peut lire toute donnée individuellement dans la mesure autorisée, mais pas toutes les données dans leur ensemble ». Le choix des critères de recherche à introduire doit exclure tout abus en situation normale. Il convient en outre de vérifier s'il n'est pas possible de contourner « l'obstacle » en obtenant d'informations complémentaires auprès d'autres sources.

C'est pourquoi la consultation en ligne de banques de données peut faire l'objet de restriction de nature à prévenir le détournement de la finalité pour laquelle les données sont rendues publiques. Ces mesures, adaptées au cas par cas, peuvent consister, par exemple, à limiter le champ d'interrogation ou les critères d'interrogation.

Ainsi, en France, les extraits d'acte de naissance sont accessibles à toute personne disposant de l'identité, de la date et du lieu de naissance d'une personne. La CNIL a subordonné la consultation en ligne de ces extraits à la condition que la demande en ligne comporte l'ensemble de ces informations. Ainsi, par la détermination de critères limitatifs d'interrogation de la base, la collecte massive de ces registres à des fins d'utilisation commerciale peut être évitée et la finalité de l'accessibilité respectée.

En France également, l'annuaire téléphonique édité sur support télématique était interrogeable à partir des premières lettres du nom, ce qui rendait plus facile son téléchargement entier et son utilisation commerciale contre la volonté de certains abonnés s'étant opposés à cet usage. Rendre impossible sur Minitel et Internet ce type d'interrogation a permis de prévenir d'éventuels détournements de finalité opérés par ce moyen.

Aux Pays bas, les CD ROM destinés à la diffusion de l'annuaire du téléphone ont été conçus de manière à empêcher l'obtention du nom et de l'adresse d'une personne à partir de la connaissance de son numéro de téléphone (l'interrogation de la base de données sur le seul champ du numéro de téléphone n'est pas possible).

De même, les bases de données relatives aux registres des entreprises ne doivent pas pouvoir être interrogées selon le critère du nom d'une personne ce qui pourrait conduire à une recherche de l'intégralité des entreprises dans lesquelles une même personne est présente.

B. Promouvoir le recours aux outils techniques tendant à empêcher la capture automatisée des données accessibles en ligne

On citera le protocole d'exclusion des moteurs de recherche (The Robots Exclusion Protocol) qui a pour objet de faire échapper à l'indexation automatisée par un moteur de recherche tout ou partie des pages d'un site. En tout état de cause, ces procédés ne pourront être efficaces que si les concepteurs de sites et les internautes sont informés de leur existence et si les moteurs de recherche les respectent. Certaines sociétés, éditrices de moteur de recherche déclarent respecter ce protocole.

III. Utilisation commerciale

Les données à caractère personnel détenues par le secteur public ont été initialement collectées et traitées à des finalités précises et, en principe, sur base d'une réglementation. Parfois la collecte était obligatoire, parfois une condition pour accéder à un service publique. Le citoyen concerné ne s'attend donc pas forcément à ce que les données le concernant soient rendues publiques et utilisées à des fins commerciales. C'est pourquoi, entre autre, certaines législations nationales permettent l'accès tout en interdisant l'utilisation commerciale des informations émanant du secteur public y compris les données à caractère personnel [1].

Du point de vue de la directive 95/46/CE [2], la question se pose de savoir si l'utilisation commerciale doit être considérée comme une finalité incompatible avec la finalité pour laquelle les données ont été collectées initialement et, dans l'affirmatif, sous quelle condition l'utilisation commerciale pourrait néanmoins être envisagée.

Si la publication et la commercialisation des informations émanant du secteur public sont admise [3], il faut respecter certaines règles et, partant, se poser la question au cas par cas de savoir comment effectivement concilier le respect du droit à la vie privée avec les intérêts commerciaux des opérateurs.

La directive 95/46/EC reconnaît un droit à la personne concernée d'être informée du traitement de ses données ainsi qu'au minimum un droit de s'opposer à des traitements légitimes. Les personnes doivent donc être informées de la finalité de commercialisation et pouvoir s'opposer à une telle utilisation par des moyens simples et efficaces [4].

Sur ce point, de nombreux progrès sont encore à faire. La multiplicité des sources de diffusion des données, le grand nombre d'opérateurs, la faculté de téléchargement, conduisent à défendre l'idée d'un guichet unique de protection des données évitant aux personnes d'avoir à accomplir à de multiples reprises la même démarche auprès de l'ensemble des opérateurs. Tel est le cas, dans plusieurs de nos pays, pour les annuaires des abonnés au téléphone.

C'est la raison également pour laquelle, la CNIL [5] a recommandé que tous les éditeurs d'annuaires identifient sur tous les supports de publication des annuaires (papier, CD-Rom, Minitel ou Internet) les abonnés qui ont exercé leur droit de s'opposer à l'utilisation de leurs coordonnées à des fins commerciales.

Cette idée de guichet unique paraît essentielle, tant pour le respect des droits exercés par les personnes, que pour les opérateurs commerciaux souhaitant utiliser des données à caractère personnel.

La conciliation du droit à la vie privée et des intérêts commerciaux des opérateurs pourrait également conduire à ce que le consentement de la personne [6], voire même des mesures législatives ou réglementaires soient nécessaires tel que l'illustre l'exemple suivant :

1 Voir Annexe 1 du livre vert : Situation actuelle dans les Etats membres en ce qui concerne la législation et les politiques relatives à l'accès à l'information émanant du secteur public, page 21 et suivantes.
2 Voir article 6 paragraphe 1 b de la directive 95/46/EC.
3 Il convient de noter que certains estiment que, étant donné que la réunion de diverses données permet d'établir des profils de personnalité, il faudrait interdire l'utilisation commerciale des données à caractère personnel ou du moins la limiter et sanctionner les infractions. En ce qui concerne les données à caractère personnel tirées de sources officielles, il ne devrait y avoir aucune exception à l'obligation d'informer la personne concernée (article 11 de la directive).
4 Voir articles 10, 11 et 14 de la directive 95/46/EC.
5 Commission Nationale des Libertés et de l'Informatique, France.
6 Voir les articles 2 h), 7a et 8 de la directive 95/46/EC concernant la définition de « consentement » ainsi que l'exigence de formes spécifiques de consentement selon le cas

Dans un avis relatif à la commercialisation des données issues des permis de bâtir, la Commission de la protection de la vie privée belge a estimé qu'une nouvelle finalité (à savoir la commercialisation des traitements des autorités publiques) pour être licite, doit être légitimée par un fondement légal ou réglementaire qui définit de manière suffisamment précise cette nouvelle finalité. A défaut, d'une telle légitimation, la Commission a estimé que l'intérêt qui est servi par la communication des données à des tiers ne l'emporte pas sur le droit au respect de la vie privée de la personne dont les données sont communiquées. Une troisième possibilité consiste en l'obtention du consentement de l'intéressé pour la finalité de commercialisation. Ce consentement doit être donnée indubitablement et en connaissance de cause en tenant compte du fait que celui qui souhaite obtenir un permis de bâtir est obligé d'introduire un dossier qui réponde à certaines prescriptions.

Plus loin dans le même avis, la Commission belge fait état de l'information des personnes en insistant plus particulièrement sur l'existence d'un droit d'opposition sur demande et gratuitement si les données ont été obtenues à des fins de marketing direct.

Conclusion :

Le législateur, lorsqu'il souhaite qu'une donnée soit rendue accessible au public n'entend pas pour autant qu'elle devienne une *res nullius*. Telle est la philosophie de l'ensemble de nos législations. Le caractère public d'une donnée à caractère personnel, qu'il résulte d'une réglementation ou de la volonté de la personne concernée elle-même, ne prive pas, ipso facto et à jamais, la personne de la protection que lui garantit la loi en vertu des principes fondamentaux de défense de l'identité humaine.

Dans le débat mené dans le cadre de la consultation sur le livre vert et dans les conclusions qui en seront tirées, il convient donc de tenir compte notamment des aspects et questions suivants en vue de concilier le respect du droit à la vie privée et à la protection des données à caractère personnel des citoyens avec le droit du public d'accéder aux informations émanant du secteur public :

— l'appréciation au cas par cas de la question de savoir si une donnée à caractère personnel peut être publiée/accessible ou non, si oui dans quelles conditions et sur quel support (numérisation ou non, diffusion sur Internet ou non etc.),
— les principes de finalité et de légitimité,
— l'information de la personne concernée,
— le droit d'opposition de la personne concernée,
— l'utilisation des nouvelles technologies pour contribuer au respect du droit à la vie privée.

Ces quelques idées directrices semblent s'imposer non seulement dans les situations dans lesquelles une réglementation concernant la publicité ou l'accès existe, mais encore dans celles où des mesures réglementaires ne paraissent pas être nécessaires en vue de satisfaire la demande formulée par le public d'accéder aux informations émanant du secteur public y compris des données à caractère personnel [1].

Dans l'attente des conclusions que tirera la Commission européenne de la consultation en cours, le Groupe exprime d'ores et déjà son grand intérêt à continuer à contribuer aux travaux envisagés dans ce domaine ainsi qu'aux questions dépassant le cadre stricte du livre vert concernant la mise à disposition de tiers des informations émanant du secteur public [2].

1 Voir note en bas de page 2.
2 Voir par exemple supra concernant le point 56 (page 9 du livre vert) sur les possibilité de collecte et de partage d'informations ainsi que le point 123 (page 19) portant sur des propositions d'action pour l'échange d'information entre entités du secteur public.

5085/99/EN/FINAL WP 25

RECOMMANDATION 3/99 RELATIVE À LA PRÉSERVATION DES DONNÉES DE TRAFIC PAR LES FOURNISSEURS DE SERVICES INTERNET POUR LE RESPECT DU DROIT

Adoptée le 7 septembre 1999

Introduction

La lutte contre la criminalité liée à l'informatique requiert de plus de plus l'attention des enceintes internationales [1]. Les pays du G8 [2] ont adopté un plan d'action [3] en dix points actuellement mis en œuvre avec l'aide d'un sous-groupe spécialisé dans la criminalité « high-tech » et composé de représentants d'agences du G8 mandatés pour faire respecter la loi. Une des questions en suspens et parmi les plus controversées concerne la conservation des données de trafic historiques et futures par les prestataires de services Internet aux fins de respect du droit et la divulgation de ces données auprès des autorités mandatées pour ce faire. Le sous-groupe du G8 pour la criminalité « high-tech » entend proposer des recommandations visant à garantir la possibilité de sauvegarder et divulguer les données de trafic. Les ministres de la justice et de l'intérieur du G8 pourraient débattre de ces recommandations lors d'une réunion qui doit se tenir à Moscou les 19 et 20 octobre 1999.

Le groupe de la protection des personnes à l'égard du traitement des données à caractère personnel [4] est conscient du rôle important que peuvent jouer les données de trafic dans le contexte des enquêtes sur les crimes perpétués sur Internet, mais souhaite toutefois rappeler aux gouvernement nationaux les principes régissant la protection des droits et libertés fondamentaux des personnes physiques, et en particulier de leur vie privée et du secret de leur correspondance qui doivent être pris en compte dans ce contexte.

Le groupe entend que les ministres de la justice et de l'intérieur du G8 pourraient être invités à préconiser une interprétation équilibrée des deux directives [5] de l'UE relatives à la protection des données au stade de la mise en œuvre, interprétation qui s'efforcera de concilier les intérêts du législateur et le droit au respect de la vie privée.

1 Voir par exemple « COMCRIME Study » « Aspects juridiques de la criminalité informatique dans la société de l'information COMCRIME Study, janvier 1997 — produite dans le cadre du plan d'action de l'UE contre le crime organisé. consulter sur le site Internet du Legal Advisory Board : http://www2.echo.lu/legal/en/comcrime/sieber.html. Le Conseil de l'Europe travaille à un projet de convention sur la criminalité informatique. Le Conseil de l'UE a exprimé son soutien pour ces travaux le 27 mai 1999. La criminalité informatique vise l'ensemble des délits commis sur les réseaux, ainsi les attaques d'ordinateur, la publication de documents illicites sur les sites Internet, de même que les activités criminelles commises par les délinquants internationaux organisés (par exemple trafiquants de drogue, activités à caractère pornographique impliquant des enfants).

2 Le G8 rassemble les pays suivants : Canada, France, Allemagne, Italie, Japon, Royaume-Uni, États-Unis d'Amérique et Russie.

3 » Réunion des ministres de la Justice et de l'Intérieur des Huit, 9-10 décembre 1997, Communiqué, Washington D.C. 10 décembre, Annexe du communiqué : Principes et plan d'action pour combattre la criminalité « high tech » « .

4 Institué par l'article 29 de 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, JO L 281 du 23.11 1995, p. 31. Disponible sur le site : http://europa.eu.int/comm/dg15/en/médias/dataprot/loi/index. htm

5 Directive 95/46/CE voir note de bas de page 3 et 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, JO L 24 du 30 janvier 1998, p. 1. Disponible sur : voir note de bas de page 4.

Le groupe est également conscient du fardeau qui peut être imposé aux opérateurs de télécommunications et aux prestataires de services.

L'objectif de la présente recommandation est donc de contribuer à une application uniforme des directives 95/46/CE et 97/66/CE de façon à ce que l'environnement dans lequel opèrent les opérateurs de télécommunications et prestataires de services Internet soit clair et prévisible, à ce que les autorités chargées de l'ordre public bénéficient du même environnement, tout en veillant à préserver le droit au respect de la vie privée.

Situation juridique

Au sein de l'Union européenne, la directive 95/46/CE harmonise les conditions de protection du droit au respect de la vie privée telles que celles-ci sont inscrites dans les législations des États membres. Cette directive se veut l'incarnation et le prolongement des principes contenus dans la Convention européenne de sauvegarde des droits de l'homme du 4 novembre 1950 et dans 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. La directive 97/66/CE particularise les dispositions de cette directive dans le secteur des télécommunications. Les deux directives s'appliquent au traitement des données personnelles, et notamment aux données de trafic relatives aux abonnés et utilisateurs sur Internet [1].

En particulier, les articles 6, 7, 13, 17 (1) et (2) de la directive 95/46/CE et les articles 4, 5, 6 et 14 de la directive 97/66/CE traitent de la légitimité de ce traitement par les opérateurs de télécommunications et prestataires de services.

Ces dispositions autorisent les opérateurs de télécommunications et prestataires de services de télécommunications à traiter les données du trafic de télécommunications sous certaines conditions très strictement définies.

L'article 6 (1) alinéa b) prévoit que les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. L'article 6 (1) alinéa e) dispose qu'elles doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. L'article 13 autorise les États membres à limiter la portée notamment de l'article 6 (1) lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sécurité de l'État, la sécurité publique ou encore la prévention, la recherche, la détection et la poursuite d'infractions pénales.

L'application de ces principes est spécifiée plus avant aux articles 5 et 6, paragraphes 2 à 5 de la directive 97/66/CE. L'article 5 garantit la **confidentialité des communications** au moyen d'un réseau public de télécommunications ou de services de télécommunications accessibles au public. Les États membres interdisent à tout autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, paragraphe 1.

En règle générale, les **données relatives au trafic** doivent être effacées ou rendues anonymes dès que la communication est terminée (article 6, paragraphe 1 de la directive 97/66/CE) Cette exigence est motivée par la sensibilité des données relatives au trafic, lesquelles révèlent des profils de communication individuels

1 Voir « Document de travail : traitement des données à caractère personnel sur Internet », adopté le 23 février 1999, disponible à : voir note de bas de page 1.

incluant les sources d'information et la localisation géographique de l'utilisateur de téléphones fixes ou mobiles et les risques potentiels pour la vie privée résultant de la collecte, de la divulgation, ou des utilisations ultérieures de ces données. Une exception est faite à l'article 6 (2) concernant le traitement de certaines données relatives au trafic dans le but d'établir les factures des abonnés et aux fins des paiements pour interconnexion, mais un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

L'article 14 (1) autorise les États membres à limiter la portée des obligations et des droits prévus à l'article 6, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales comme le prévoit l'article 13, paragraphe 1 de la directive 95/46/CE.

Il résulte de ces dispositions que les opérateurs de télécommunications et fournisseurs de services Internet ne sont pas autorisés à recueillir et stocker des données uniquement aux fins du respect de la loi, à moins que celles-ci ne leur en fassent obligation pour les motifs et sous les conditions mentionnées ci-dessus. Ceci est conforme aux traditions depuis longtemps en vigueur dans la plupart des États membres où l'application des principes de protection des données nationales a entraîné l'interdiction pour le secteur privé de conserver les données à caractère personnel au seul motif d'une possible nécessité ultérieure exprimée par la police ou les forces de sécurité de l'État.

Dans ce contexte, on peut noter qu'aux fins du respect de la loi et aux conditions visées aux articles 13 de la directive 95/46/CE et 14 de la directive 97/66/CE, une législation existe dans la plupart des États membres, définissant les conditions précises dans lesquelles les forces de police et de sécurité de l'État peuvent avoir *accès* aux données stockées par des opérateurs de télécommunications et prestataires de services Internet privés pour leurs propres besoins civils.

Comme le groupe de protection l'a déjà indiqué dans sa recommandation 2/99 relative au respect de la vie privée dans le contexte de l'interception des télécommunications, adoptée le 3 mai 1999 [1], le fait qu'une tierce partie vienne à prendre connaissance de données relatives au trafic concernant l'utilisation de services de télécommunications a généralement été considéré comme une interception de télécommunications, et constitue donc une violation du droit de l'individu au respect de sa vie privée et de la confidentialité de la correspondance telle que garantie par l'article 5 de la directive 97/66/CE [2]. De surcroît, une telle divulgation de données relatives au trafic est incompatible avec l'article 6 de cette directive.

Toute violation de ces droits et obligations est inacceptable à moins de répondre à trois critères fondamentaux, conformément à l'article 8 (2) de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, et à l'interprétation de cette disposition par la Cour européenne des droits de l'homme : une base juridique, la nécessité de cette mesure dans une société démocratique et la conformité à un des objectifs légitimes énumérés dans la Convention. La base juridique doit définir précisément les limites et les moyens d'application de la mesure : les objectifs pour lesquels les données peuvent être traitées, la durée pendant laquelle celles-ci peuvent être conservées (éventuellement) et l'accès à celles-ci doivent être strictement limités. Une surveillance exploratoire à

1 Disponible sur : voir note de bas de page 1.
2 Les services autorisés exigent également l'accès aux informations sur les connexions en temps réel, données concernant les connexions actives (« données relatives au trafic futures »).

grande échelle ou générale doit être prohibée [1]. Il s'ensuit que les administrations publiques ne peuvent se voir octroyer l'accès aux données relatives au trafic qu'au cas par cas et jamais de façon anticipée ou en règle générale.

Ces critères coïncident avec les dispositions susmentionnées aux articles 13 de la directive 95/46/CE et 14 de la directive 97/66/CE.

Divergence des règles nationales [2]

En ce qui concerne la période durant laquelle les données relatives au trafic peuvent être stockées, la directive 97/66/CE n'autorise la conservation qu'à des fins de facturation [3] et uniquement jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée. Cependant, cette période varie sensiblement suivant les États membres. En Allemagne par exemple, les opérateurs de télécommunications et prestataires de services de télécommunications sont autorisés à stocker les données nécessaires à la facturation pendant un délai pouvant aller jusqu'à 80 jours aux fins de prouver l'exactitude de la facturation [4]. En France, tout dépend du statut de l'opérateur : l'opérateur de télécommunications « traditionnel » est autorisé à conserver les données relatives au trafic pendant un maximum d'un an sur la base de la loi fixant la période durant laquelle la facture peut être contestée. Cette période est fixée à dix ans pour les autres opérateurs. En Autriche, la loi sur les télécommunications ne fixe pas de période concrète maximale pendant laquelle les données relatives au trafic peuvent être stockées aux fins de la facturation, mais la limite est la période durant laquelle la facture peut être contestée ou des poursuites engagées pour en obtenir le paiement. Au Royaume-Uni, la loi prévoit que la facture peut être contestée pendant six ans, mais les opérateurs et prestataires de services conservent les données correspondantes pendant environ dix-huit mois. En Belgique par exemple, la loi ne définit pas une telle période, mais le plus grand prestataire de services de télécommunications a fixé cette période à trois mois dans ses conditions générales. Une autre pratique peut être observée au Portugal où, la période n'étant pas fixée par la loi, l'autorité nationale de supervision de la protection des données décide au cas par cas. Il est intéressant de noter qu'en Norvège, la période est fixée à quatorze jours.

1 Voir spécialement l'arrêt Klass du 6 septembre 1978, série A n° 28, pages.23 et suivantes et l'arrêt Malone du 2 août 1984, série A n° 82, pages 30 et suivantes.
L'arrêt Klass, de même que l'arrêt Leander du 25 février 1987, insiste sur la nécessité de « garanties effectives contre les abus » « compte tenu du risque qu'un système de surveillance secrète destiné à la protection de la sécurité nationale pose pour ce qui est d'hypothéquer, voire de détruire la démocratie au motif de défendre celle-ci ». (Arrêt Leander, série A n° 116, pages 14 et suivantes).
La Cour observe dans l'arrêt Klass (paragraphes 50 et suivants) qu'évaluer l'existence d'une garantie adéquate et effective contre les abus dépend de toutes les circonstances de l'affaire. Dans le cas d'espèce, elle considère que les mesures de surveillance prévues par la législation allemande n'autorisent pas de surveillance exploratoire ou générale et ne contreviennent pas à l'article 8 de la convention européenne pour la protection des droits de l'homme. La législation allemande prévoit les garanties suivantes : la surveillance est limitée aux cas dans lesquels on dispose d'indications permettant de soupçonner une personne de projeter, de commettre ou d'avoir commis certains actes criminels graves ; des mesures ne peuvent être ordonnées que si l'établissement des faits par une autre méthode s'avère sans perspectives de réussite ou présente des difficultés beaucoup plus considérables ; et même dans ces circonstances, la surveillance ne peut s'appliquer qu'aux suspects spécifiques ou à ses « personnes de contact » présumées.
2 La Commission analyse actuellement les législations des États membres qui ont communiqué les mesures nationales d'application des directives 97/66/CE et 95/46/CE. Voir le tableau d'application concernant la directive 95/46/CE disponible sur : voir note de bas de page 4.
3 Et, le cas échéant, pour les paiements d'interconnexion entre opérateurs de télécommunications, voir article 6 paragraphe 2 de la directive 97/66/CE.
4 Si la facture est contestée durant cette période, les données pertinentes peuvent bien entendu être conservées jusqu'au règlement du différend.

La pratique courante des PSI n'est elle non plus pas homogène : il semble que les petits PSI conservent les données relatives au trafic pendant des périodes très courtes (quelques heures) en raison d'une pénurie de capacités de stockage. Les PSI plus importants qui peuvent se permettre de telles capacités de stockage peuvent conserver les données relatives au trafic pendant une durée pouvant aller jusqu'à quelques mois (mais ceci dépend de leurs politiques tarifaires : par durée de connexion ou par période fixe).

Pour le respect de la loi, la loi néerlandaise sur les télécommunications oblige les opérateurs et prestataires de services de télécommunications à collecter et stocker les données relatives au trafic pendant trois mois.

Obstacles au fonctionnement du marché intérieur

Cette divergence soulève des obstacles potentiels au sein du marché intérieur pour ce qui de la fourniture transfrontière de services de communication et Internet, mais de même de telles périodes divergentes peuvent contrarier le respect effectif de la loi. On peut arguer du fait qu'un PSI établi dans un État membre n'est pas habilité à stocker des données relatives au trafic pendant un laps de temps supérieur à celui fixé dans l'État membre où le client vit et utilise le service. Ou bien un PSI peut subir une pression visant à le faire conserver des données relatives au trafic plus longtemps que cela n'est autorisé dans son propre État membre du fait qu'il s'agit d'une exigence du pays des utilisateurs. En cas de facturation pour appels hors secteur local dans le domaine de la téléphonie mobile, ce n'est pas l'opérateur étranger qui recouvre la facture, mais l'opérateur national des abonnés concernés. Différentes périodes pour le stockage des données nécessaire à la facturation peuvent ainsi conduire aux mêmes problèmes que ceux décrits pour les PSI. La règle de la loi applicable exposée à l'article 4 de la directive 95/46/CE ne résout ce problème que dans la mesure où le PSI est le contrôleur et établi uniquement dans un État membre, mais non dans les cas où celui-ci est établi dans plusieurs États membres pour lesquels les périodes sont différentes ou lorsque celui-ci traite des données relatives au trafic au nom du contrôleur.

Recommandation

Compte tenu de ce qui précède, le groupe de travail considère que le moyen le plus efficace de réduire des risques inacceptables pour la vie privée tout en reconnaissant la nécessité d'une application efficace de la loi voudrait que les données relatives au trafic ne soient pas en principe uniquement conservées à des fins de respect de la loi et que les législations nationales n'obligent pas les opérateurs de télécommunications, les fournisseurs de services de télécommunications et de services Internet à conserver des données relatives au trafic pendant une période plus longue qu'il n'est nécessaire à des fins de facturation.

Le groupe recommande que la Commission européenne propose des mesures appropriées visant à mieux harmoniser la période pendant laquelle les opérateurs de télécommunications, prestataires de services de télécommunications et de service Internet sont autorisés à conserver des données relatives au trafic à des fins de facturation et de paiement liés à l'interconnexion [1]. Le groupe considère que cette période devrait être aussi longue que nécessaire pour permettre aux consommateurs de contester la facturation, mais aussi courte que possible de façon à ne pas surchar-

1 Compte tenu de cet objectif, il n'y a pas de justification à opérer de distinctions entre opérateurs privés ou publics.

ger les opérateurs et prestataires de services et de manière à respecter les principes de proportionnalité et de spécificité entrant dans le cadre du droit au respect de la vie privée. Cette période devrait être alignée sur la norme la plus élevée de protection observée dans les États membres. Le groupe attire l'attention sur le fait que dans plusieurs États membres, des périodes n'excédant pas trois mois ont été appliquées avec succès.

Le groupe recommande d'autre part que les gouvernements nationaux tiennent compte des considérations ci-dessus.

5007/00/FR/FINAL

AVIS 1/2000 SUR CERTAINS ASPECTS DU COMMERCE ÉLECTRONIQUE RELATIFS À LA PROTECTION DES DONNÉES PRÉSENTÉ PAR LA TASK FORCE INTERNET
Adopté le 3 février 2000

Introduction

L'UE est en passe d'adopter une proposition de directive sur certains aspects juridiques du commerce électronique [1]. Comme il l'a fait jusqu'à présent, le Groupe de travail « Article 29 » sur la protection des données [2] a l'intention d'apporter une contribution constructive à ce renforcement du cadre juridique pour le commerce électronique. Par cet avis, le Groupe de travail souhaite également mettre en évidence un problème de protection des données soulevé par le commerce électronique et expliquer comment il est traité dans la législation européenne. Le cadre juridique pour la protection du droit fondamental à la vie privée et la protection des données à caractère personnel est déjà en place sous la forme de la directive 95/46/CE définissant les principes généraux de la protection des données et de la directive 97/66/CE complétant ceux-ci pour le secteur des télécommunications.

Le Groupe de travail se félicite de la clarification expresse, apportée dans un nouveau considérant et un nouvel article 1 (4) (b), concernant l'application correcte et intégrale de la législation relative à la protection des données [3] dans les services Internet. Cela signifie que la mise en œuvre de la directive sur le commerce électronique doit se faire en parfait conformité avec les principes de la protection des données.

Le Groupe de travail a déjà accordé beaucoup d'attention aux problèmes de protection des données soulevés par Internet, notamment en 1999, en proposant des orientations générales concernant trois questions importantes relatives aux caractéristiques spécifiques des nouvelles technologies de l'information. Il a émis un avis sur

1 Proposition modifiée de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, COM (1999) 427 final. Un accord politique sur un texte a été trouvé lors du Conseil des ministres du 7 décembre 1999 ; une position commune sera bientôt officiellement adoptée avant une deuxième lecture au Parlement européen. Voir communiqué de presse IP/99/952 p. 1 et 4.
2 Établi par l'article 29 de la directive 95/46/CE, citée dans la note 3 ci-dessous.
3 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281/31 du 23 novembre 1995 et directive 97/66 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, JO L 241/1 du 30 janvier 1998, toutes deux disponibles sur : http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.h tm

l'information émanant du secteur public [1] et des recommandations sur le traitement invisible et automatique des données à caractère personnel sur Internet [2], ainsi que sur la conservation des données relatives au trafic par les prestataires de services Internet en vue de l'application du droit [3]. Dans le contexte du commerce électronique, une quatrième question se pose. Le Groupe de travail voudrait à présent donner une interprétation sur l'application des règles européennes en matière de protection des données au traitement des données pour les besoins du publipostage électronique.

La question du publipostage électronique

Afin de pouvoir lancer une campagne de publicité ou de publipostage commercial, une entreprise doit acquérir une liste importante et appropriée d'adresses de courrier électronique de clients potentiels. Elle peut acquérir ces adresses par Internet de trois manières : par la collecte directe auprès des clients ou visiteurs de sites web, en se procurant des listes préparées par des tiers [4] et par la collecte à partir d'espaces publics sur Internet tels que des répertoires publics, des forums de discussion ou des espaces de dialogue.

Une caractéristique des publipostages commerciaux par voie électronique est que si le coût pour l'émetteur est extrêmement faible comparé aux méthodes traditionnelles de marketing direct, il existe un coût pour le destinataire en termes de temps de connexion. Cette situation en matière de coût crée une incitation claire à utiliser cet outil de marketing à grande échelle et à négliger les préoccupations relatives à la protection des données et les problèmes causés par le publipostage électronique.

Du point de vue du citoyen, le problème est triple : premièrement, la collecte de l'adresse électronique d'une personne sans son consentement ou à son insu, deuxièmement la réception de grandes quantités de publicités non sollicitées et, troisièmement, le coût du temps de connexion. Dans ce domaine, un problème majeur est le « spamming » [5], qui désigne l'envoi massif — et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics d'Internet. Le problème, du point de vue du marché intérieur, est la possibilité d'avoir des réglementations nationales divergentes en matière de communication commerciale par voie électronique qui créent des barrières au commerce. Les deux types de problèmes ont influencé l'élaboration de la législation communautaire dans ce domaine.

1 Avis 3/99 concernant l'information émanant du secteur public et la protection des données à caractère personnel, adopté le 3 mai 1999 : WP20 (5055/99). Tous les documents adoptés par le Groupe de travail sont disponibles sur : http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/inde x.htm
2 Recommandation 1/99 sur le traitement invisible et automatique des données à caractère personnel sur l'Internet effectué par des moyens logiciels et matériels, adoptée le 23 février 1999 : WP 17 (5093/98).
3 Recommandation 3/99 sur la conservation des données relatives au trafic par les prestataires de services Internet en vue de l'application du droit, adoptée le 7 septembre 1999 : WP 25 (5085/99)
4 Les listes préparées par un tiers peuvent être établies sur la base de données collectées directement auprès de clients ou sur la base de données collectées dans des espaces publics sur Internet.
5 Ce sujet a été traité par le Rapport sur le publipostage électronique et la protection des données personnelles adopté par la CNIL le 14 octobre 1999, disponible sur www.cnil.fr. Les parties 2 et 3 de cet avis se fondent en partie sur ce rapport.

La législation communautaire et son application au publipostage électronique

Le principe général selon lequel la législation relative à la protection des données s'applique au commerce électronique a déjà été abordé [1]. Le publipostage électronique est un exemple spécifique de la manière dont les problèmes de protection des données soulevés par le courrier électronique peuvent être résolus en appliquant les principes juridiques contenus dans les deux directives. La directive générale stipule que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [2]. Le traitement ne peut être effectué que si la personne concernée a donné son consentement, s'il est nécessaire à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde de l'intérêt vital de la personne, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ou à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée [3]. De plus, la personne doit être informée des finalités du traitement auquel les données sont destinées [4], et se voir reconnaître le droit de s'opposer au traitement des données à caractère personnel la concernant à des fins de marketing direct [5]. La directive sur la protection de la vie privée dans le secteur des télécommunications donne aux États membres le choix entre appliquer une solution « opt-in » (garantie de consentement) ou une solution « opt-out » (droit d'opposition) pour les communications commerciales non sollicitées [6]. Aux règles de la protection des données sont ajoutées certaines exigences inspirées par la protection des consommateurs. La directive sur la vente à distance requiert, par exemple, qu'au minimum les consommateurs se voient accorder le droit de refuser la communication à distance [7] opérée au moyen du courrier électronique.

La directive relative au commerce électronique pourrait, une fois adoptée, prévoir à l'article 7 une disposition explicite concernant deux aspects *techniques :* l'obligation d'identifier le courrier électronique commercial en tant que tel et l'obligation de consulter et de respecter les registres d'opposition lorsqu'ils sont prévus par les règlements nationaux (solution opt-out). Mais un considérant et l'article 1 (4) (b) indiquent clairement que cette directive n'a nullement pour objet de modifier les principes et les exigences *juridiques* contenus dans le cadre législatif existant décrit plus haut. Étant donné que la législation relative à la protection des données s'applique pleinement au commerce électronique, la mise en œuvre de la directive relative au commerce électronique doit être parfaitement conforme aux principes de la protection des données. Cela signifie premièrement qu'en ce qui concerne la protection des données, le droit national applicable à une entreprise responsable du traitement de données à caractère personnel restera celui de son pays d'établissement dans l'UE [8]. Cela signifie également que la directive relative au commerce électronique ne peut ni

1 Document de travail : Traitement des données à caractère personnel sur l'Internet. Adopté le 3.2 1999 : WP 16 (5013/99)
2 Directive 95/46/CE, article 6
3 Directive 95/46/CE,. article 7
4 Directive 95/46/CE, article 10
5 Directive 95/46/CE,. article 14
6 Directive 97/66/, article 12. L'usage du courrier électronique pour le marketing direct peut même être assimilé à celui des automates d'appels, pour lesquels un consentement est requis.
7 Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, JO L 144/19 du 4 juin 1997, article 10 (le courrier électronique est expressément inclus en vertu de l'article 2 (4) et de l'annexe 1) ; disponible sur http://www.europa.eu.int/eur-lex/en/lef/dat/1997/en_397L0007.html
8 Directive 95/46/CE, article 4.

empêcher les États membres d'imposer aux entreprises de demander le consentement préalable pour les communications commerciales [1], ni empêcher l'utilisation anonyme d'Internet [2].

Selon le groupe de travail, ces règles apportent une réponse claire aux problèmes de protection de la vie privée soulevés dans la partie 2 ci-dessus et définissent clairement les droits et obligations des acteurs concernés. Deux situations doivent être distinguées :

Si une adresse électronique est collectée par une entreprise *directement auprès d'une personne,* en vue d'un publipostage électronique par cette entreprise ou un tiers auquel les données sont communiquées, l'entreprise initiale doit informer la personne de ces finalités au moment de la collecte de l'adresse [3]. La personne dont les données sont collectées doit également, au minimum, se voir accorder, au moment de la collecte et à tout moment par la suite, le droit de s'opposer à l'exploitation de ses données personnelles par des moyens électroniques simples tels que cliquer dans une case prévue à cet effet, par l'entreprise initiale et par toutes les entreprises qui ont reçu les données de l'entreprise initiale [4]. Certaines lois nationales appliquant les directives concernées exigent même de l'entreprise qu'elle obtienne le consentement de la personne au sujet de laquelle des données sont collectées. Les exigences de l'article du projet de directive sur le commerce électronique concernant les communications commerciales non sollicitées compléteraient ces règles au niveau technique en imposant au prestataire de services l'obligation de consulter un registre mais n'enlèveraient rien des obligations générales applicables aux personnes responsables du traitement des données.

Si une adresse électronique est collectée dans un *espace public sur Internet,* son utilisation pour le publipostage électronique serait contraire à la législation communautaire applicable et ceci, pour trois raisons. D'abord, elle pourrait être considérée comme un traitement « illicite » de données à caractère personnel au titre de l'article 6 (1) (a) de la directive générale. Ensuite, elle serait contraire au principe de finalité de l'article 6 (1) (b) de cette directive dans la mesure où la personne concernée a communiqué son adresse de courrier électronique pour une tout autre raison, par exemple pour participer à un forum de discussion. Troisièmement, compte tenu du déséquilibre des coûts et du dérangement occasionné au destinataire, ces envois pourraient être considérés comme ne satisfaisant pas au test de l'équilibre d'intérêt de l'article 7 (f) [5].

Conclusions

Le présent avis ne doit nullement être considéré comme la position finale du Groupe de travail sur l'interaction entre le commerce électronique et la protection des données. Son but est de renforcer la sensibilisation aux problèmes soulevés par un type particulier de traitement de données qui fait actuellement l'objet d'un débat dans différentes sphères, et de contribuer à la compréhension du cadre juridique applicable au commerce électronique. Au-delà des aspects déjà abordés par le Groupe de travail, il pourrait y avoir d'autres problèmes liés au commerce électronique qui nécessitent une interprétation ou une approche commune. Aussi, le Groupe de travail

1 Voir article 12 de la directive 97/66/CE.
2 Voir considérant 6a de la proposition modifiée, note 1 ci-dessus.
3 Directive 95/46/CE, article 10
4 Directive 95/46/CE, article 14
5 Cette disposition (l'un des motifs légitimes du traitement) prévoit que le traitement doit être « nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement… à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée,… »

considère qu'il est nécessaire d'élaborer une politique commune sur certains aspects tels que le cyber-marketing, les paiements électroniques et les technologies améliorant la protection de la vie privée. Il a demandé à sa Task force Internet de poursuivre ces travaux. Différents résultats sont attendus, notamment des recommandations de mesures techniques relatives au « spam » ou à la validation des sites web sur la base d'une liste de contrôle européenne commune conforme aux directives relatives à la protection des données.

CA07/434/00/FR WP 32
Traduction extérieure non révisée

AVIS 4/2000 SUR LE NIVEAU DE PROTECTION ASSURÉ PAR LES « PRINCIPES DE LA SPHÈRE DE SÉCURITÉ »
Adopté le 16 mai 2000

Introduction

Le présent avis est diffusé en référence aux principes de la sphère de sécurité et aux questions souvent posées (FAQ) que les services de la Commission ont transmis les 28 avril et 2 mai ainsi qu'en référence à d'autres documents reçus entre le 9 et le 11 mai.

Le groupe de travail considère que des progrès importants et significatifs visant à l'amélioration de la protection des données à caractère personnel ont été réalisés au cours des deux années de négociation avec le ministère américain du commerce et qu'une dernière série d'avancées pourrait être réalisée sur un nombre limité de questions fondamentales. Il remarque notamment que les dernières modifications apportées aux principes et aux documents connexes intègrent plusieurs suggestions apportées par le groupe de travail dans ses avis précédents.

Lors de l'élaboration de son avis, le groupe de travail a également pris en compte la « réponse du ministère américain du commerce » à son avis 7/99 [1], reçue par fax le 26 avril.

Le groupe de travail rappelle que la protection des personnes à l'égard du traitement des données à caractère personnel fait partie des « droits et libertés fondamentaux » : cette dimension, qui est déjà inscrite dans la Convention européenne des droits de l'homme et qui est rappelée à l'article premier de la directive 95/46, est confirmée par l'orientation émanant du travail de la Convention sur la Charte européenne des droits fondamentaux. Le groupe de travail réaffirme que, pour être jugé adéquat, un système de protection des données doit répondre aux critères résumés dans son document de travail (WP 12) du 24 juillet 1998.

Il rappelle également que les Etats-Unis ont signé les lignes directrices de l'OCDE sur la vie privée (1980) et réaffirmé leur soutien à ces dernières lors de la conférence ministérielle d'Ottawa de 1998.

Le groupe de travail souhaite mettre en évidence les répercussions de la directive 95/46 dans le contexte international. Le groupe de travail mesure l'importance économique et commerciale l'ensemble des dispositions afférent à la sphère de

1 Tous les documents cités dans le présent avis peuvent être obtenus sur demande auprès du secrétariat du groupe de travail.

sécurité. Il est toutefois convaincu que ces considérations ne peuvent pas l'emporter sur les droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel. En outre, il importe de ne pas perdre de vue les conséquences de toute constatation d'un niveau adéquat de protection pour des négociations futures dans le cadre de forums internationaux tels que l'OMC. Le groupe de travail approuve la déclaration faite dans le projet de lettre des services de la Commission au ministère américain du commerce, qui précise que le système juridique des Etats-Unis présente des caractéristiques très particulières et ne peut pas être considéré comme un précédent : le groupe de travail partage la préférence des services de la Commission pour des règles contraignantes dont la directive et les lignes directrices de l'OCDE restent les principales références.

Le groupe de travail a déjà commenté toutes les versions provisoires publiées aux divers stades de ce dialogue. Le groupe de travail a notamment diffusé les avis suivants [1] :
— avis 1/99 du 26 janvier 1999 (WP 15) ;
— avis 2/99 du 3 mai 1999 (WP 19) ;
— avis 4/99 du 7 juin 1999 (WP 21) complété par le document de travail du 7 juillet 1999 (WP 23) ;
— avis 7/99 du 3 décembre 1999 (WP 27).

Après avoir examiné la nouvelle version des documents reçus les 28 avril et 2 mai, le groupe de travail confirme son précédent avis et considère qu'il est essentiel de prendre dûment en considération les questions et les recommandations ci-dessous.

Portée

Droit applicable

Dans son avis 7/99, le groupe de travail a insisté sur les malentendus qui pourraient éventuellement résulter du principe de la notification et s'est montré préoccupé par la possibilité, pour les responsables du traitement des données, de dénaturer les principes de la sphère de sécurité en supplantant la législation des Etats membres. Le groupe de travail a par conséquent proposé de clarifier cette question dans une FAQ spécifique. Cette suggestion n'a pas été suivie et l'amendement du paragraphe 2 des principes a été modifié d'une manière qui n'apporte pas d'éclaircissement sur cette question (version du 28 avril). Toutefois, dans sa « réponse » à l'avis 7/99, le ministère américain du commerce précise que « la législation européenne va manifestement régir tous les aspects de la collecte et de l'utilisation des informations à caractère personnel par les sociétés opérant en Europe ». Le groupe de travail rappelle qu'en vertu de la directive (article 4.1), les Etats membres sont tenus d'appliquer les dispositions nationales qu'ils arrêtent, non seulement lorsque les données sont traitées par les responsables du traitement sur leur territoire, mais aussi lorsque les responsables (bien que non établis sur leur territoire) recourent à des moyens situés sur ledit territoire, en particulier pour la collecte de données à caractère personnel. Le groupe de travail invite la Commission à préciser, dans le projet de décision ou dans la lettre au ministère du commerce, que les dispositions de la sphère de sécurité ne portent pas préjudice à l'application de l'article 4 de la directive.

1 Tous les documents adoptés par le groupe de travail sont disponibles à l'adresse suivante : http://europa.eu.int/comm/internal _market/en/media/dataprot/wpdocs/index.htm

Transferts de données ne relevant pas de la compétence d'un organe de type « FTC »

Selon le projet de décision établi par les services de la Commission (article 1.1.b), les organisations américaines qui souhaitent bénéficier des avantages de la sphère de sécurité doivent relever de la compétence d'un organe de type FTC. L'adhésion aux principes de la sphère de sécurité étant fondée sur l'autocertification, sans aucune sorte de vérification ex-ante, les pouvoirs de contrôle d'un organisme public sont essentiels à la crédibilité de la construction.

Dans son avis 7/99, le groupe de travail a déjà fait remarquer que, selon les lettres que la FTC a adressées aux services de la Commission, seules les pratiques commerciales déloyales ou frauduleuses relèvent de la compétence de la FTC et que des secteurs tels que les services financiers (banques et assurances), les télécommunications, le transport, les relations de travail et les activités non lucratives n'entrent pas dans ses attributions. Le groupe de travail accepte donc le nouveau libellé du projet de décision de la Commission (article 1.1, point b), en vertu duquel une nouvelle annexe 3 énumérera les organismes publics américains répondant aux critères de l'article 1.1, point b, et admet que les secteurs où les traitements qui ne relèvent pas des organismes cités ne peuvent entrer dans le champ d'application de la décision (cf. comme énoncé au 9ème considérant).

D'autre part, le groupe de travail constate que, dans la version des principes du 28 avril, les organisations non soumises à la loi sur la « Federal Trade Commission » peuvent encore prétendre aux avantages de la sphère de sécurité sans être clairement tenues d'autocertifier leur engagement auprès du ministère du commerce et considère qu'il est nécessaire de lever cette ambiguïté en rajoutant les passages supprimés.

Pour ce qui est de la FAQ 13 (réservation de passagers des transports aériens), le groupe de travail a examiné le projet de lettre (du 9 mai) élaboré par le ministère des transports et note que celui-ci mentionne la possibilité de recours individuels ainsi que l'intention de notifier toute action entreprise au ministère du commerce. En l'état actuel des choses, le groupe de travail ne s'oppose donc pas à l'inclusion du ministère des transports dans la liste dont il est fait référence à l'article 1.1., point b, pour autant que les conditions exposées à l'article 1 du projet de décision soient respectées.

En ce qui concerne les données sur l'emploi, le groupe de travail fait remarquer que la FAQ 6, dans la version du 28 avril, dispose que « si les organisations souhaitent que les avantages de la sphère de sécurité couvrent les informations concernant les ressources humaines (...) elles doivent l'indiquer dans leur lettre et s'engager à coopérer avec l'autorité européenne (...) conformément aux FAQ 9 et 5 ». Toutefois, la réponse à la première question de la FAQ 9 établit que « les principes de la sphère de sécurité ne s'appliquent qu'aux transferts des fichiers identifiés individuellement. Le groupe de travail rappelle que, conformément à la directive, les principes de la sphère de sécurité définissent les données à caractère personnel comme des données relatives à des personnes identifiées ou identifiables et considère que la FAQ 9 doit être mise en conformité avec la bonne définition. En outre, le groupe de travail s'inquiète du fait que la mise en œuvre des dispositions relatives aux données sur l'emploi ne repose que sur la coopération des autorités chargées de la protection des données plutôt que sur celle des autres organes de règlement des litiges.

Fusions, rachats et faillites

D'une manière générale, les dispositions législatives s'appliquent à toute organisation établie sur le territoire d'un pays ou d'un Etat donné. Les règles de la « sphère de sécurité » ne s'appliqueront qu'aux organisations dont l'adhésion aux principes a été volontaire, ce qui soulève des questions spécifiques, résumées par le groupe de travail

dans son avis 7/99. Le groupe apprécie les améliorations apportées à la FAQ 6 (nouveau paragraphe ajouté le 28 avril). La « nouvelle économie » enregistre chaque jour des fusions, des rachats et des faillites. Dans son avis 7/99 (page 3), le groupe de travail avait invité la Commission à envisager la suppression ou l'effacement des données qui avaient été transférées à des organisations qui avaient adhéré aux principes et n'existent plus et se réjouit que cette proposition ait été prise en compte.

Exceptions

• Le groupe de travail déplore que les normes de la sphère de sécurité soient affaiblies, d'une part, par des exceptions introduites par les « questions souvent posées » et, d'autre part, par le paragraphe 5 des principes (« l'adhésion aux principes peut être limitée… par les textes législatifs, les règlements administratifs ou la jurisprudence qui créent des obligations contradictoires ou des autorisations explicites »).

En ce qui concerne le dernier point, le groupe de travail répète [1] que l'adhésion aux principes ne devrait être limitée que dans la mesure nécessaire pour respecter des obligations contradictoires et que, pour des raisons de transparence et de sécurité juridique, le ministère américain du commerce devrait avertir la Commission de tout texte législatif ou règlement administratif qui affecterait l'adhésion aux principes. Les autorisations explicites motivant des exceptions ne peuvent être acceptées que si les intérêts légitimes supérieurs qui sous-tendent ces autorisations ne s'écartent pas de façon sensible des exemptions ou des dérogations accordées par les Etats membres de l'UE dans des situations comparables en application des lois nationales mettant en œuvre la directive.

En ce qui concerne les exceptions visées dans les FAQ, le groupe de travail émet l'avis suivant :

• Données mises à la disposition du public (FAQ 15) : le groupe de travail répète qu'une exception pour les données mises à la disposition du public et les fichiers publics n'est pas conforme aux instruments internationaux relatifs à la protection des données et notamment aux lignes directrices de l'OCDE [2]. Il constate qu'une nouvelle formulation a été introduite et pourrait contribuer à éviter des cas d'exemption abusive, mais déplore que l'on n'ait pas tenté de définir plus précisément la catégorie d'informations couvertes. En outre, le groupe de travail rappelle que l'ensemble des dispositions afférent à la sphère de sécurité ne peut ni déroger au cadre juridique régissant les questions de responsabilité (qu'il s'agisse du droit coutumier ou du droit civil) ni établir que « les organisations ne pourront être tenues pour responsables » (comme indiqué au paragraphe 3 de la réponse à la FAQ 15, qui devrait par conséquent être supprimé) ;

• Accès (FAQ 8) : le groupe de travail confirme les objections déjà répétées dans son avis 7/99 (pages 8 et 9) à l'encontre de la longue liste d'exceptions créées par la section 5. Par la même occasion, le groupe de travail observe que des objections similaires ont été énoncées dans la proposition du Dialogue transatlantique des consommateurs (TACD) [3].

1 Avis 7/99, page 4
2 Des principes applicables aux données à caractère public ont été élaborés par le groupe de travail « Article 29 » dans son avis 3/99, adopté le 3 mai 1999, en ce qui concerne l'information émanant du secteur public et la protection des données à caractère personnel.
3 Proposition du TACD, page 4 : « Les exceptions en matière de fourniture d'accès sont trop générales et limitent injustement l'accès des personnes au profit des intérêts commerciaux. Si d'autres considérations doivent être prises en compte avec les droits d'accès, les principes d'accès actuels permettent aux entités les moins susceptibles de prendre en considération les droits de la personne concernée à savoir les responsables de la collecte des données d'effectuer cette détermination » (_).

Le groupe de travail considère que le recours aux exceptions devra être strictement contrôlé et qu'il faut rechercher la coopération des autorités américaines afin de s'assurer que les exceptions ne soient pas utilisées dans le but d'ébranler la protection garantie par les principes. Le groupe de travail estime notamment que, dans un système adéquat de protection des données, le droit d'accès ne peut être limité ni refusé de façon incompatible avec la directive.

Principes

Accès

Le principe de la sphère de sécurité ne prévoit pas le droit de recevoir des données « sous une forme aisément intelligible », bien que ce droit soit reconnu par les lignes directrices de l'OCDE (« principe de la participation individuelle »). Le groupe de travail pend note que le ministère américain du commerce soutient (dans sa réponse à l'avis 7/99) que ce droit est sous-entendu par le principe.

Le principe d'accès donne le droit de supprimer des données uniquement si elles sont inexactes et non si elles sont collectées ou traitées sans l'accord de la personne concernée ou d'une manière incompatible avec les principes. Dans le dernier cas, l'obligation de supprimer les données, comme l'a recommandé le groupe de travail dans son avis 7/99, est désormais l'une des « sanctions possibles » de la section « recours et sanctions » de la FAQ 11. Plutôt que de confier la responsabilité de supprimer les données aux organes alternatifs de règlement des litiges (comme indiqué par la note de bas de page correspondante de la FAQ 11), le groupe de travail recommande de reconnaître le droit de suppression comme un droit individuel ou d'en faire une obligation pour les organisations qui adhèrent à la sphère de sécurité.

Choix

En ce qui concerne les modifications de l'utilisation des données, la possibilité de faire opposition est actuellement offerte aux personnes concernées lorsque les informations à caractère personnel sont utilisées dans un but incompatible avec l'objectif initial de la collecte. Ce principe doit être élargi afin de couvrir toutes les utilisations différentes des données à caractère personnel.

En outre, la possibilité de faire opposition telle qu'elle est offerte par le principe de choix doit être étendue aux transferts de données à d'autres organismes, même si l'usage qui est fait des données ou le but recherché reste inchangé. Le groupe de travail accueille favorablement la norme actuelle de choix explicite pour les données sensibles, mais juge qu'il est nécessaire de définir les données concernées de façon claire et absolue. La dernière phrase du principe de choix doit être clarifiée : il convient de remplacer l'expression « en tout cas » par « en outre ». De plus, le groupe de travail recommande de préciser davantage encore le principe de finalité et la notion de choix.

Transferts ultérieurs

La version actuelle des principes de la sphère de sécurité autorise des transferts à des tiers qui n'observent pas les principes de la sphère de sécurité si ces derniers s'engagent par écrit à protéger les données. Cette approche n'est pas compatible avec les règles générales visant à garantir la mise en œuvre de la sphère de sécurité et la responsabilité des organisations qui y adhèrent. Dans ces conditions, le groupe de travail considère que les transferts ultérieurs doivent être soumis au consentement des personnes concernées.

Mise en œuvre

Comme le rappellent la directive (article premier) et la Convention européenne des droits de l'homme, le droit à la vie privée est un droit fondamental (article 8) et toute personne a le droit d'être entendue par un organe indépendant. La « sphère de sécurité » permettra le transfert des données à caractère personnel, actuellement traitées au sein de l'Union européenne, vers un pays dans lequel les garanties susmentionnées ne s'appliquent peut-être pas. Par conséquent, la question essentielle est de savoir comment, dans le cas des données transférées vers les Etats-Unis, le droit fondamental à la vie privée sera protégé si les principes de la « sphère de sécurité » ne sont pas appliqués.

Conformément à la dernière version des documents américains, la mise en œuvre des principes reposerait sur deux niveaux :
— le règlement alternatif des litiges (bien qu'il semble que les organismes existants, cités par les États-Unis, couvrent uniquement des activités « en ligne » : BBB online, Webtrust et Trust-e) ;
— les pouvoirs d'injonction de la « Federal Trade Commission » qui ont été expliqués dans trois lettres distinctes de la présidence de la FTC.

Le « lien » entre ces deux niveaux est extrêmement incertain : aux termes de la FAQ 11, les organes alternatifs de règlement des litiges devraient signaler à la FTC les cas où les principes ne sont pas respectés, mais rien ne les y oblige. Même si les personnes concernées peuvent se plaindre directement à la FTC, il ne peut être garanti que la FTC examinera leur affaire (ses pouvoirs étant discrétionnaires). Concrètement, les personnes concernées n'auront pas le droit d'être entendues par la FTC, ni pour appliquer ni pour contester les décisions prises par les organes alternatifs de règlement des litiges (ou l'absence de telles décisions). Par conséquent, les personnes concernées par une violation supposée des principes ne seront pas assurées de pouvoir se présenter devant une instance indépendante [1].

Le projet d'aide-mémoire du ministère américain du commerce évoque la possibilité d'actions individuelles devant les tribunaux américains et d'indemnisations pour préjudice moral ; l'expérience montre que de telles indemnisations sont fréquemment accordées en cas de violation du droit à la vie privée. Ces deux aspects devront être examinés à la lumière de l'expérience acquise de façon à s'assurer de l'efficacité des solutions exposées dans l'aide-mémoire susmentionné.

D'une manière générale, le groupe de travail estime que les dispositions de ce régime de mise en œuvre présentent des lacunes pour deux des trois conditions indiquées dans son document de travail du 24 juillet 1998 (page 7) : le besoin d'« apporter soutien et assistance aux personnes concernées » (lettre b) et « de fournir des voies de recours appropriées à la partie lésée en cas de non respect des règles » (lettre c).

Conclusions

Le groupe de travail constate que la proposition relative à la « reconnaissance » d'un niveau adéquat de protection fait référence à un système qui n'est pas encore opérationnel. À cet égard, le groupe de travail approuve la clause de révision

1 En vertu de la proposition susmentionnée du Dialogue transatlantique des consommateurs, bien que « la vie privée individuelle ait été précédemment compromise, aucun groupe autorégulateur n'a jamais demandé d'investigation sur une société membre » : dans ses conclusions, le TACD recommande que « les négociateurs de la sphère de sécurité considèrent la disposition d'un droit individuel de recours comme une priorité ».

figurant dans le projet de décision de la Commission qui permet d'examiner, à la lumière de l'expérience acquise, toute reconnaissance du niveau adéquat de protection assuré par la sphère de sécurité ; en outre, le groupe de travail estime qu'il doit réaffirmer son avis 7/99 concernant la « période de grâce » et confirme sa réserve sur cette partie du projet d'échange de lettres (le groupe de travail fait observer que le projet de lettre des services de la Commission fait référence aux « extraits joints des comptes rendus du Comité 'Article 31' » — qui ne sont pas encore disponibles — et souhaiterait recevoir ce document).

Après avoir examiné l'ensemble des éléments susmentionnés, et en tenant compte de l'engagement américain relatif à la protection de la vie privée tel qu'il est exposé dans la « réponse » du ministère du commerce à l'avis 7/99, le groupe de travail reste préoccupé par un certain nombre de domaines dans lesquels, selon lui, la protection des données pourrait être améliorée. Le groupe de travail souhaite en particulier une amélioration de la situation afin d'aboutir à :

— une clarté absolue quant au champ d'application de la sphère de sécurité, d'une part, en termes de droit applicable et, d'autre part, en termes de compétence de la FTC (chapitre 1 du présent avis) ;

— une limitation des exceptions et exemptions conformément aux indications visées au chapitre 2 du présent avis ;

— d'autres améliorations des principes telles qu'elles sont exposées au chapitre 3 ;

— des garanties appropriées de voies de recours individuelles, tel qu'indiqué au chapitre 4.

Si une décision devait être prise de poursuivre, le groupe de travail mettrait en particulier l'accent sur la valeur des mécanismes permettant de réexaminer la décision et sur d'autres garanties.

Enfin, et indépendamment de la décision à adopter en ce qui concerne la « sphère de sécurité », le groupe de travail encourage les services de la Commission à finaliser leur travail et à présenter une décision sur les clauses contractuelles types (article 26.4 de la directive) afin de créer un cadre prévisible, sûr et non discriminatoire pour les transferts internationaux de données qui ne se limitent pas à un seul pays tiers. En outre, le groupe de travail invite la Commission à envisager en priorité la création d'un système de label européen pour les sites Internet, basé sur des critères communs d'évaluation de la protection des données déterminables au niveau communautaire.

Table des matières

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