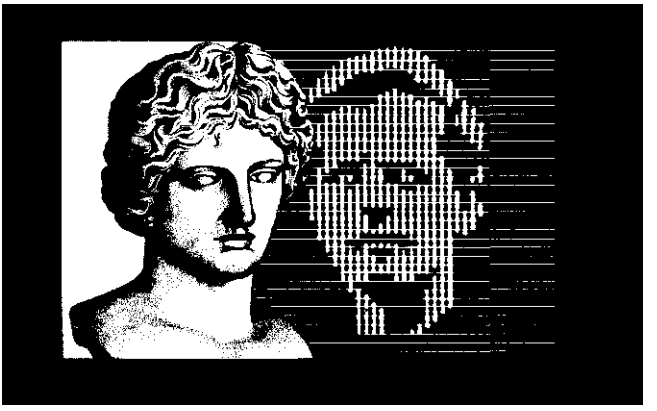
18e rapport d'activité 1997

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS



Edition 1998

La documentation Française

CNIL

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

18e rapport d'activité 1997

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

ISBN 2-11-004033-5

Sommaire

Avant-propos

La publication de ce rapport intervient quelques mois après le 20e anniversaire de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et quelques mois avant la transposition en droit français de la directive européenne du 24 octobre 1995 sur la protection des personnes à l'égard du traitement des données à caractère personnel. Ce dix-huitième rapport d'activité de la CNIL n'est pas pour autant un rapport de transition.

L'année 1997 demeurera en effet celle de nombreuses avancées d'une société de l'information respectueuse des règles de protection des données personnelles, tout particulièrement en ce qui concerne Internet.

La Commission Nationale de l'Informatique et des Libertés avait, dès 1995, souligné les risques inhérents à l'utilisation qui pourrait être faite du gisement de données personnelles que constitue Internet. Il s'agissait alors de la diffusion sur Internet d'annuaires de chercheurs. En 1996, la CNIL avait appelé l'attention sur le phénomène de la traçabilité des données relatives aux internautes qui naviguent sur le Net.

Inspirés d'un souci de réalisme, les travaux de la Commission sur ces questions se sont depuis lors considérablement enrichis, notamment en ce qui concerne l'ouverture de sites ministériels sur Internet, le développement du commerce électronique ou les traitements d'informations nominatives mis en œuvre par les fournisseurs d'accès au réseau.

Ces travaux lui ont permis de se forger la conviction qu'une des clés de la réussite d'Internet réside dans la capacité qu'aura le réseau à respecter les droits des personnes, tout particulièrement le droit à la vie privée des internautes qui accèderont à Internet en toute confiance lorsqu'ils auront acquis la certitude

que les cyber-consommateurs et les cyber-citoyens ne sont pas inéluctablement des objets de surveillance.

Le site internet de la CNIL, innovant et pédagogique lorsqu'il fait la démonstration du pistage des internautes sur le réseau, vient de recevoir le « dauphin d'or » des sites web des collectivités et institutions lors du dernier festival de Biarritz. Cette récompense confirme que la démarche de la Commission sur Internet est la bonne. Ce prix atteste à tout le moins que cette méthode de sensibilisation reçoit un excellent écho chez les professionnels de la communication et de l'informatique appliquée au multimédia.

Ces interventions et réflexions de la Commission relatives à Internet et aux flux transfrontières d'informations nominatives s'inscrivent dans un contexte national et un environnement international en pleine mutation.

Ainsi la CNIL se félicite que le programme d'action du gouvernement tendant à préparer l'entrée de la France dans la société de l'information fasse toute sa place au souci de la protection des données personnelles. La Commission se félicite également, et ce rapport en rend compte, d'avoir été invitée à faire, à la suite du rapport de M. Guy Braibant, des suggestions au gouvernement dans le cadre des travaux liés à la transposition en droit français de la directive européenne du 24 octobre 1995.

Au plan international, la CNIL est le témoin actif, parfois même l'inspirateur, de nombreuses initiatives qui sont autant de signes que cette société de l'information, par nature mondiale, ne fera pas l'impasse sur la protection des données personnelles. Puisse une vigilance de tous et de tous les instants conduire un jour à apaiser définitivement les craintes telles que celles formulées par M. Tim Bemers-Lee, créateur du World Wide Web en 1989, qui se déclarait récemment « *très inquiet des conséquences sur la vie privée de l'utilisation du Net ».*

Ce dix-huitième rapport annuel dresse évidemment le bilan des autres activités de la Commission Nationale de l'Informatique et des Libertés tant en ce qui concerne l'examen des fichiers informatiques avant leur mise en oeuvre que le contrôle a posteriori de ces fichiers à travers l'instruction des plaintes, l'exercice du droit d'accès indirect ou les visites sur place.

Parmi les questions évoquées dans ce rapport, les recommandations et les avis émis par la CNIL à propos des mégabases de données comportementales, des annuaires téléphoniques de nouvelle génération ou encore de la montée en charge du dispositif Sesam-Vitale, attestent que l'informatique peut demeurer au service de chaque citoyen et qu'il est toujours possible de conjuguer progrès technique et liberté.

Jacques Fauvet

L'ORGANISATION ET LE FONCTIONNEMENT DE LA COMMISSION

I. LA COMPOSITION

La Commission est composée de dix-sept membres nommés pour cinq ans ou pour la durée de leur mandat.

Cette composition a connu plusieurs changements au cours de l'année 1997 et au début de l'année 1998 :
- Monsieur Charles Renard a été élu par la Cour des comptes pour siéger à la CNIL en remplacement de Monsieur Michel May, décédé en mars 1997 ;
- à la suite des élections législatives de juin 1997, l'Assemblée nationale a désigné Messieurs Raymond Forni et Gérard Gouzes pour succéder à Messieurs Christian Dupuy et Philippe Houillon ;
- Monsieur Noël Chahid-Nouraï a été élu par l'assemblée générale du Conseil d'État en remplacement de M^{me} Louise Cadoux, vice-président délégué.

Les modifications intervenues dans la composition de la Commission, notamment la démission de M^{me} Cadoux, ont conduit la CNIL à procéder à un renouvellement partiel de son bureau. Ont été désignés, à l'issue d'une élection organisée le 17 mars 1998 :
- M. Michel Benoist comme vice-président délégué.
- M. Raymond Forni comme vice-président.

Figurent en annexe du rapport :
- la composition de la Commission (annexe 1) ;
- la répartition des secteurs d'activité entre ses membres (annexe 2).

II LES MOYENS ET LES SERVICES

En 1997, les crédits alloués à la CNIL au titre du budget voté s'élevaient à 30 321 769 francs. Ces crédits ont été ramenés à 30 052 693 francs pour 1998, compte tenu notamment d'une importante économie réalisée par la Commission sur ses dépenses de loyers.

Budget voté	1996	**1997**	1998
Rémunération des personnels	15 735 849	**16 752 141**	17 237 622
Vacations et autres rémunérations	2 794 983	2 **802 816**	3 429 497
Fonctionnement	11 319812	**10 766 812**	9 385 574
Total et variation / à l'exercice précédent	29 850 644 (- 0,48 %)	**30 321 769** (+ **1,58 %)**	30 052 693 (- 0,89 %)

L'organigramme des services, qui n'a connu aucun changement notable en 1997, est présenté en annexe 3.

Première partie

LES CHIFFRES, LES TEXTES ET L'ACTIVITÉ EUROPÉENNE ET INTERNATIONALE

Chapitre 1

L'ANNÉE 1997

EN CHIFFRES

En 1997, la Commission a tenu vingt-cinq séances plénières et adopté 97 délibérations dont la liste est publiée en annexe 4.

I. LES VISITES SUR PLACE ET LES CONTRÔLES

Dans le cadre de ses missions d'information, de concertation et de contrôle a *priori* et a *posteriori* de l'informatique appliquée aux traitements de données nominatives, la CNIL a procédé à près de quarante visites sur place en 1997. Elle a en outre décidé, par délibération, d'effectuer vingt et une missions de contrôle.

Le compte rendu des principales visites et missions de contrôle apparaît dans les deuxième et troisième parties du rapport, respectivement consacrées aux enjeux pour l'année 1997 et à l'intervention de la CNIL dans les différents secteurs de la vie publique, économique et sociale.

II. LES FORMALITES PREALABLES À LA MISE EN ŒUVRE DES TRAITEMENTS

A. Bilan

1978-1997

Le nombre total de traitements enregistrés par la CNIL depuis 1978 est, au 31 décembre 1997, de **575 71**7 dont :
- déclarations simplifiées et modèles types : 408 864 (71,02 % du total) ;
- demandes d'avis : 31 245 (5,43 % du total) ;
- déclarations ordinaires : 135 608 (23,55 % du total).

Le nombre de demandes de déclaration de modification de traitements enregistrés depuis 1978 est de 24 226.

Comme les années précédentes, ces chiffres confirment l'importance du recours par les déclarants aux procédures simplifiées mises en œuvres par la Commission pour la déclaration des traitements.

1997

Pour la période du 1er janvier au 31 décembre 1997, la CNIL a enregistré **67 136** nouveaux dossiers de formalités préalables dont :
- déclarations simplifiées et modèles types : 53 953 (80,36 % du total) ;
- demandes d'avis : 2 724 (4,06 % du total) ;
- demandes d'autorisation (recherche médicale) : 133 (0,20 % du total) ;
- déclarations ordinaires : 10 326 (15,38 % du total).

Elle a reçu 2 639 déclarations de modification de traitements déjà enregistrés, ce qui a porté à 69 **775** le nombre de nouveaux dossiers à instruire.

Une comparaison avec l'année 1996 permet de constater une diminution sensible du nombre de dossiers de formalités préalables reçus par la CNIL (-9,29 %). Cette baisse, notamment en ce qui concerne les traitements du secteur public, traduit sans doute une anticipation sur l'allégement des procédures de déclaration des traitements informatiques qui devrait selon toute vraisemblance résulter de la transposition de la directive européenne du 24 octobre 1995 (cf. 17e rapport, p. 27 et *infra* 1re partie, chapitre 2).

	1996	1997	variation
Déclarations simplifiées et modèles types	60 355	53 953	- 10,60 %
Demandes d'avis	3 269	2 724	-16,67 %
Déclarations ordinaires	9 727	10 326	+ 6,15 %
Déclarations de modification	3 428	2 639	-23,01 %
Total	76 779	69 642	- 9,29 %

B. Normes simplifiées et modèles types

1) LES 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 simplifiée. Élaborées en vertu du pouvoir réglementaire détenu par la Commission, ces normes visent à alléger les procédures de déclaration.

À titre de rappel, 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 du traitement à la norme, la CNIL peut inviter le. déclarant à justifier de cette conformité 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.

Ainsi la CNIL a reçu, en 1997, 53 953 déclarations de conformité à une norme simplifiée ou à un modèle type.

Au cours de l'année, la Commission a édicté une nouvelle norme simplifiée relative à la gestion des instruments financiers, ce qui porte à quarante et une le nombre de normes simplifiées adoptées depuis 1978. Par ailleurs, dans le souci d'étendre le bénéfice de cette simplification des procédures, la CNIL a procédé en 1997 à la modification d'une norme existante.

La norme simplifiée n° 41 relative à la gestion des instruments financiers

Afin d'encourager les opérateurs du marché financier français à déclarer les fichiers qu'ils mettent en œuvre, la CNIL a adopté une norme simplifiée relative à la gestion des instruments financiers. Cette norme, qui est le fruit d'une vaste concertation avec les professionnels des marchés financiers et des services d'investissement, prend en compte les pratiques et la modernisation de ce secteur d'activité consacrée par la loi du 2 juillet 1996, qui a notamment procédé à la transposition en droit français de la directive européenne sur les services d'investissements. Ce texte a redéfini les instruments financiers et réorganisé le marché financier français ; il a en outre créé la notion d'entreprise d'investissement, appelée à remplacer celles de société de bourse, d'agent des marchés interbancaires et de gestionnaire de portefeuille ; enfin, il a créé une autorité professionnelle unique, le Conseil des marchés financiers (CMF), qui se substitue au Conseil des bourses de valeurs et au Conseil du marché à terme.

À la lumière de ce cadre juridique rénové, il a semblé utile de simplifier les déclarations de traitements que des opérateurs tant français qu'étrangers sont amenés à constituer sur le territoire national. Ainsi, la norme simplifiée n° 41 adoptée par délibération n° 97-066 du 9 septembre 1997, publiée au *Journal*

officiel du 1er octobre 1997, recense les fonctionnalités des traitements concernés, les catégories d'informations traitées, leurs destinataires et la durée de conservation des données.

Délibération n° 97-066 du 9 septembre 1997 concernant les traitements automatisés d'informations nominatives relatifs aux instruments financiers

(Norme simplifiée n° 41)

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 ;

Vu la loi n° 96-597 du 2 juillet 1996 de modernisation des activités financières ;

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

Considérant que la CNIL est habilitée, en vertu des articles 6, 17 et 21 (1) de la loi du 6 janvier 1978 susvisée, 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 les traitements automatisés portant sur la gestion d'instruments financiers sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné ;

Décide :

Article 1er

Les dispositions de la présente délibération concernent les traitements automatisés d'informations nominatives relatifs aux instruments financiers mis en œuvre par les prestataires de services d'investissement tels que définis par l'article 6 de la loi n° 96-597 du 2 juillet 1996 susvisée.

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée de conformité à la présente norme 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 — Finalités du traitement

Le traitement doit avoir pour seules fonctions :
a) l'enregistrement, la mise à jour et l'exploitation des informations concer nant les inscriptions en compte et les caractéristiques du fonctionnement de ces comptes ;
b) le suivi des activités relatives aux instruments financiers ;
c) la gestion des opérations effectuées sur ces comptes, avec les émetteurs d'instruments financiers et les prestataires de services d'investissement au sens de la loi n° 96-597 du 2 juillet 1996 ;
d) la gestion des opérations effectuées pour le compte de l'État, des émetteurs publics ou privés auprès des détenteurs d'instruments financiers, associés, actionnaires, administrateurs, obligataires, rentiers ou porteurs de parts, de droits ou de bons ;
e) l'exécution des obligations fiscales ;
f) la gestion des différentes formes de participation, d'intéressement des salariés et d'actionnariat.

Article 3 — Catégories d'informations traitées

Dès lors que les dispositions de l'article 27 de la loi n° 78-17 du 6 janvier 1978 ont été respectées lors du recueil des informations traitées, celles-ci doivent relever seulement des catégories suivantes :
a) identité : nom, prénoms, adresse (s) postale (s), adresse domicile, adresse fiscale, sexe, date et lieu de naissance, identité bancaire, nationalité, pays de l'adresse fiscale principale, statut de résident ;
b) situation familiale : éléments sur la situation matrimoniale nécessaire à la tenue du compte ;
c) catégorie socioprofessionnelle ou profession ;
d) caractéristiques du compte et de l'instrument financier :
- nature du compte ;
- garanties ;
- limites d'utilisation du compte et conditions financières ;
- valeurs nominales ;
- prix d'émission ;
- date de jouissance ;
- délais de mise à disposition ;
- forme de titres ;
- statut fiscal ;
- date de négociation ;
- désignation de la valeur négociée ;
- quantité de titres en dépôt ;
- virements fiscaux ;
- revenus d'instruments financiers ;
- gains et pertes ;
- montants soumis à double imposition ;

- quantité de valeurs mobilières négociées ;
- portefeuille titres ;
- capacité de placement ;
- cours de bourse ;
- informations spécifiques relatives à la gestion des différentes formes d'épargne salariale y compris l'actionnariat des salariés : salaires, montant des droits.

e) Informations en rapport avec la justice : capacité juridique.

Article 4 — Destinataires des informations

Peuvent seuls dans les limites de leurs attributions respectives être destinataires de certaines des informations :
- les personnels habilités chargés de la tenue des comptes ;
- les supérieurs hiérarchiques de ces personnels ;
- les agents habilités des établissements liés contractuellement pour l'exécution de tâches se rapportant à la gestion d'instruments financiers et des espèces ;
- les agents habilités des autres établissements teneurs de comptes pour les transferts de fonds ;
- les agents habilités des façonniers, entreprises extérieures liées contractuellement pour l'exécution de certaines tâches matérielles ;
- les auxiliaires de justice et officiers ministériels dans le cadre de leurs missions ;
- les agents habilités de la direction générale des impôts du Trésor public, de la Banque de France, des divers organismes publics habilités à les recevoir ;
- les agents habilités des autorités de tutelle, publiques ou privées, et des services chargés du contrôle (commissaires aux comptes, audit, services chargés des procédures internes ou externes de contrôle).

Article 5 — Durée de conservation

Les informations nominatives nécessaires aux traitements automatisés tels que définis aux articles 1er, 2 et 3 ne doivent pas être conservées au-delà de la durée prévue par la réglementation en vigueur et notamment par l'article 16 du code de commerce relatif à la durée de conservation des livres et documents créés à l'occasion d'activités commerciales, sous réserve des dispositions relatives à la prescription trentenaire.

Article 6 — Enregistrements et traitements complémentaires

Les traitements dont les finalités sont celles définies à l'article 2 ci-dessus qui comportent l'enregistrement d'informations n'appartenant pas aux catégories énumérées à l'article 3 ou aboutissant à la transmission d'informations à des destinataires autres que ceux définis à l'article 5 doivent faire l'objet, selon qu'ils relèvent de l'article 15 ou de l'article 16 de la loi du 6 janvier 1978 susvisée, d'une demande d'avis ou d'une déclaration ordinaire.

La modification de la norme simplifiée n° 20 relative au patrimoine immobilier à caractère social

Afin de l'adapter au cadre juridique actuel en matière de gestion du logement social, qui vise notamment à réserver ce type d'habitat aux plus démunis, la CNIL a modifié la norme simplifiée n° 20 qu'elle avait adoptée par une délibération n° 81 -53 du 26 mai 1981.

La nouvelle norme n° 20, publiée au *Journal officiel* du 13 mars 1997, a un champ d'application plus étendu que la précédente et tient compte de la nécessité de collecter davantage d'informations pour tenir compte des critères sociaux d'attribution des logements. Cette nouvelle rédaction de la norme a été réalisée en concertation avec l'Union des HLM et le ministère du Logement.

Les finalités des traitements prévus par la norme ont été élargies au recouvrement des impayés, à l'élaboration de statistiques issues de certaines enquêtes obligatoires, aux opérations nécessaires à l'organisation des élections des représentants de locataires au conseil d'administration (établissement des listes électorales...).

Conformément aux textes législatifs et réglementaires en vigueur, de nouvelles informations peuvent être collectées dans le cadre de cette norme ; il s'agit de la nature et de la durée de validité d'un titre de séjour dans la mesure où le bénéfice de ces logements a été ouvert aux personnes admises à séjourner régulièrement sur le territoire français ainsi que d'un certain nombre d'informations concernant la vie professionnelle (catégorie socio-professionnelle, coordonnées de l'employeur, inscription à l'ANPE...), les ressources (avis d'imposition...) ou encore la situation de famille qui inclut désormais la date du dernier changement de fait ou de droit de la situation matrimoniale. Enfin, peuvent désormais être collectées des informations relatives à un handicap ou aux motifs de la demande d'attribution d'un logement, le temps de l'instruction du dossier. Dans tous les cas, lorsqu'une demande n'a pas de suite favorable, les informations relatives aux demandeurs, et le cas échéant, aux motifs de cette demande, que le logement ait été ou non attribué, ne peuvent pas être conservées au-delà d'un an à compter de la date de dépôt de la demande.

La liste limitative des destinataires des données a été complétée et vise désormais de nouveaux organismes tels que les services du Trésor chargés du recouvrement des loyers ou encore le fonds de solidarité pour le logement.

Délibération n° 97-005 du 21 janvier 1997 concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social

(Norme simplifiée n° 20)

La Commission nationale de l'informatique et des libertés, Vu les articles 6, 17 et 21 (1) de la loi n° 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 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 du patrimoine immobilier à caractère social sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 susmentionné ;

Décide :

Article 1er

Les dispositions de la présente décision concernent les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social mis en oeuvre par les organismes publics ou privés.

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) de permettre la gestion des candidatures soit à l'attribution d'un logement locatif, soit à l'accession à la propriété ;.

b) 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 afférentes, la régularisation des charges, les pièces comptables nécessaires au recouvrement et à la gestion des comptes des locataires concernés ;

c) de permettre l'accession à la propriété et le conventionnement des logements locatifs y compris la gestion de l'aide personnalisée au logement ;

— d'opérer le contrôle des ressources des locataires d'habitations à loyer modéré et de calculer le supplément de loyer conformément aux dispositions de la loi du 4 mars 1996 ;

e) d'effectuer les opérations de réalisation des prêts à l'accession à la propriété des particuliers et de gestion de leur compte ;

f) de procéder au recouvrement des impayés ;

g) (délibération n° 84-35 du 16 décembre 1984.) « de mettre en oeuvre des politiques sociales de l'habitat définies en faveur des populations concernées » ;

h) de réaliser des enquêtes relatives à la gestion du patrimoine ainsi que des statistiques :
- d'une part, en matière d'accession à la propriété et de location ;
- d'autre part, en vue de la perception des aides financières accordées sur la base de la collecte de la participation des entreprises à l'effort de construction réservé au logement des immigrés ;
i) de permettre les opérations nécessaires à l'organisation des élections des représentants des locataires au conseil d'administration ;

Article 3 — Catégories d'informations traitées

Dès lors que les dispositions de l'article *17* de la loi n° 78-17 du 6 janvier 1978 ont été respectées lors du recueil des informations traitées, celles-ci doivent relever seulement des catégories suivantes :

a) identité : nom, nom marital, date et lieu de naissance, prénoms, (délibé ration n° 84-35 du 16 octobre 1984.) « nationalité », adresse, numéro de téléphone, code interne de traitement permettant l'identification du loca taire, du copropriétaire ou du propriétaire (à l'exclusion du numéro d'in scription au répertoire national des personnes physiques) ;

b) nature et durée de validité du titre de séjour pour permettre l'examen des conditions de recevabilité de la demande ;

c) identité bancaire ou postale ;

d) logement : caractéristiques du logement ou des biens immobiliers, assu rance, 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, montant du supplément de loyer, nature et montant des charges, des travaux d'entretien et d'amélioration, nature des prêts consentis et modalités de remboursement ;

Informations nécessaires à la gestion du patrimoine à caractère social :

Vie professionnelle :
- catégorie socioprofessionnelle (agriculteur-ouvrier-employé-technicien-a gent de maîtrise — cadre-moyen — cadre-supérieur-artisan-commerçant-pro-ression libérale-retraité-sans activité-étudiant) ;
- nature de l'activité professionnelle ;
- situation de demandeur d'emploi inscrit à l'ANPE ;
- coordonnées de l'employeur.

Ressources :
- revenus d'activité (avis d'imposition) ;
- allocations prévues par le décret n° 96 1163 du 26 décembre 1996.

Situation de famille
- situation matrimoniale ;
- état civil du conjoint et des autres personnes vivant sous le même toit, date du dernier changement de fait ou de droit de la situation matrimoniale.

f) numéro d'allocataire de la caisse d'allocations familiales exclusivement pour permettre le versement de l'aide personnalisée au logement ;

g) handicap éventuel des personnes composant le foyer pour la prise en considération de leur qualité de personne à charge dans le cadre du calcul des ressources tant pour l'attribution de logements que pour le calcul du supplément de loyer solidarité ;

h) motifs de la demande du candidat à l'attribution d'un logement au regard des dispositions des articles R. 441-3 et R. 441-4 du code de la construction et de l'habitation.

Article 4 — Durée de conservation

Les informations relatives aux locataires en place ne doivent pas être conservées après le règlement du solde de l'intéressé à l'exception des informations nécessaires à l'accomplissement des obligations légales. Toutefois les informations visées à l'article 3h ne pourront pas être conservées au-delà d'une année à compter de la date du dépôt de la demande. Les informations relatives aux demandeurs de logement ne doivent pas être conservées au-delà d'une année à compter de la date de dépôt ou de renouvellement de la demande.

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 et des prêts ;
— l'organisme financier teneur du compte courant du locataire de l'accé dant ou du propriétaire ;
— la Commission départementale de l'aide personnalisée au logement ;
— les auxiliaires de justices et les officiers ministériels dans le cadre de leur mission de recouvrement de créances ;
— les organismes payeurs des allocations de logement et de l'aide person nalisée au logement ;
— les services du Trésor chargés d'assurer le recouvrement des loyers ;
— les services des impôts chargés du recouvrement et du contrôle de la contribution annuelle sur les logements à usage locatif (article 302 bis Zc du code général des impôts) ;
— le fonds de solidarité pour le logement (FSL) (article 6 loi n° 90-449 du 31 mai 1990) ;
— les organismes chargés de la constitution d'un fichier unique de la demande de logement (article R. 441-2 alinéa 3 du CCH), les organismes regroupés au sein d'un protocole d'occupation du patrimoine social (article L. 441-2 du CCH) et les organismes participant à l'élaboration du plan départemental d'action pour le logement des personnes défavorisées (loi n° 90-449 du 31 mai 1990) ;
— les réservataires de logements HLM (article R. 441-9 du CCH) ;
— le maire de la commune où se situent les logements à attribuer en sa qualité de membre de la commission d'attribution (article L. 441-1, L. 441-1-1 et R. 441-1 du CCH).

Toutefois, peuvent seuls avoir connaissance sous une forme nominative de la nationalité ainsi que des informations relatives à la nature et à la validité du titre de séjour les destinataires mentionnés ci-dessus qui participent à la procédure d'attribution des logements.

Article 6 — Dispositions complémentaires

Les traitements dont les finalités sont celles définies à l'article ci-dessus, qui comportent l'enregistrement d'informations n'appartenant pas aux catégories énumérées à l'article 3 ou aboutissent à la transmission d'informations à des destinataires autres que ceux définis à l'article 5 doivent faire l'objet de demande d'avis ou de déclarations complémentaires selon qu'ils relèvent des articles 15 ou 16.

Article 7

La norme simplifiée instituée par la délibération n° 81-53 du 26 mai 1981 modifiée par la délibération n° 84-35 du 16 octobre 1984 est abrogée.

2) LES MODELES TYPES

L'article 29 du règlement intérieur de la CNIL 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 et, 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.

En 1997, la CNIL a adopté 8 nouveaux modèles types qui concernent :
- Le secteur protection sociale : 1
(cf. délibération n° 97-002 du 14 janvier 1997, 3e partie, chapitre 7).
- Le secteur travail : 1
(cf. délibération n° 97-037 du 27 mai 1997, 3e partie, chapitre 10).
- Le secteur justice : 3
(cf. délibération n° 97-004 du 21 janvier 1997, délibération n° 97-036 du 27 mai 1997 et délibération n° 97-056 du 30 juin 1997, 3e partie, chapitre 4).
- Le secteur santé : 2
(cf. délibération n° 97-016 du 4 mars 1997 et délibération n° 97-067 du 9 septembre 1997, 3e partie, chapitre 5).
- Le secteur administration : 1
(cf. délibération n° 97-032 du 6 mai 1997, 2e partie, chapitre 1).

Depuis 1978, 287 modèles types ont reçu un avis favorable de la Commission et 12 379 traitements ont donné lieu à des déclarations de conformité en référence à l'un de ces modèles.

C. Demandes d'avis et demandes d'autorisation

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'État (procédure jamais utilisée à ce jour). Si, au terme d'un délai de deux mois renouvelable une fois — qui, de jurisprudence constante, court à compter du jour où le dossier est complet, — l'avis de la Commission n'est pas notifié, il est réputé favorable (avis tacite).

Au cours de l'année 1997, la Commission a reçu 2 724 demandes d'avis et en a définitivement traité 2 701 dont 2 157 de l'année en cours et 544 des années antérieures. Au 31 décembre 1997, 2 015 dossiers étaient en cours d'instruction.

Parmi les 2 701 demandes d'avis traitées en 1997 :
- 52 ont donné lieu à un avis favorable ;
- 2 ont donné lieu à un avis défavorable ;
- 2 381 ont donné lieu à un avis tacite ;
- 266 ont été requalifiées en déclaration ordinaire, déclaration simplifiée, modèle type, demandes de modification, ou ont été annulées, ou ont eu leur instruction, sur la demande du déclarant, momentanément suspendue.

Depuis 1978, la CNIL a émis 88 avis défavorables, soit 0,28 % du total des demandes d'avis.

En 1997, les deux avis défavorables rendus par la CNIL concernent :
- un projet de création, par une mairie, d'une base de données fiscales et foncières destinée à informer l'administration fiscale d'éventuelles anomalies. La CNIL a rappelé que le contrôle des situations fiscales devait rester de la compétence exclusive de l'administration des impôts et que toute transmission de données fiscales à des tiers est interdite. De même, les renseignements communiqués aux services fiscaux ne peuvent pas être le résultat de l'analyse par des services municipaux de la situation des assujettis *(cf.* délibération n° 97-074 du 7 octobre 1997, 3e partie, chapitre 2) ;
- un projet d'utilisation par une mairie, des rôles des impôts locaux aux fins d'information des administrés sur la politique fiscale locale. La Commission a notamment considéré que ce projet ne respectait pas le caractère objectif qui doit présider à l'information ainsi diffusée (cf. délibération n° 97-076 du 7 octobre 1997, 3e partie, chapitre 2).

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 aux 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, dont la création doit être autorisée 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 *(cf.* 15e rapport, p. 27 et 17e rapport, p. 32 et 33).

Après une phase transitoire nécessaire à la mise en place effective du Comité, la Commission a commencé, en 1997, à se prononcer sur des dossiers dont le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé avait été préalablement saisi. La Commission a ainsi reçu, en 1997, 133 demandes d'autorisation (cf. *infra* 3e partie, chapitre 6).

Dans un souci constant d'allégement des formalités qui incombent aux organismes de recherche, la CNIL a adopté, par délibération n° 97-011 du 4 février 1997, un modèle de demande d'autorisation visant à simplifier les procédures.

Ce formulaire comporte quatre parties : la première doit présenter la finalité de la recherche et ses principales caractéristiques, la deuxième concerne les modalités d'information des personnes concernées, la troisième rend compte des caractéristiques du traitement mis en œuvre à l'occasion de la recherche, la dernière précise les mesures prises pour assurer la confidentialité des informations et la sécurité du traitement.

D. 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 1997, 10 326 déclarations ordinaires.

Il convient de relever que l'arrêt du Conseil d'État du 6 janvier 1997, a décidé que 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, le récépissé de déclaration doit être délivré sans délai, sans que la CNIL dispose d'un pouvoir d'appréciation particulier (cf. *infra* chapitre 2 et annexe 7).

À la suite de cet arrêt, la Commission a mis fin à la pratique consistant à surseoir à la délivrance de récépissés pour des dossiers qui étaient formellement complets mais qui faisaient apparaître des risques de violations manifestes de la loi du 6 janvier 1978. Il pouvait s'agir d'une durée de conservation excessive des informations ou d'un défaut de pertinence des données collectées au regard de la finalité du traitement, ou bien encore d'une collecte déloyale ou illicite au regard de l'article 25 de la loi. Parallèlement, la Commission a modifié la rédaction des récépissés de déclaration ordinaire afin qu'en aucun cas la délivrance d'un récépissé ne puisse être interprétée comme constituant un label de conformité que la CNIL décernerait aux traitements mis en œuvre dans le secteur privé.
Pour autant, cette décision ne prive nullement la CNIL de son pouvoir de dénonciation au parquet, ni de son pouvoir de délivrer des avertissements en cas de situation illégale ; aussi, la CNIL, conformément à sa mission de conseil

qu'elle tient de l'article 6 et de sa volonté de concertation, s'efforce-t-elle d'attirer l'attention d'un déclarant lorsqu'il lui apparaît que sur tel ou tel point d'un projet, la mise en œuvre du traitement serait de nature à constituer une violation de la loi du 6 janvier 1978 ou à susciter des inquiétudes de la part des personnes fichées.

III. 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 un registre des traitements déclarés, de recevoir les réclamations, pétitions et plaintes, ainsi que d'exercer, aux lieu et place des requérants, leur droit d'accès aux fichiers intéressant la sécurité publique et la sûreté de l'État.

À ce titre, la Commission répond aux demandes de conseils juridiques ou techniques qui lui sont adressées, instruit les plaintes dont elle est saisie, procède aux vérifications nécessaires dans le cadre du droit d'accès indirect et délivre à toute personne qui en fait la demande un extrait du « fichier des fichiers », c'est-à-dire du registre informatisé, tenu par la CNIL, recensant l'ensemble des traitements qui lui ont été déclaré.

A. Bilan général

La Commission a reçu, au cours de l'année 1997, 4 452 saisines qui se répartissent de la manière suivante :

Nature des saisines	1997	Pourcentage du total des saisines	Rappel 1996	Variation
Plaintes	2 348	52,74 %	2 028	+ 15,77 %
Demandes de conseil	821	18,44 %	1008	- 18,55 %
Demandes de radiation des fichiers commerciaux	263	5,91 %	277	- 5,05 %
Demandes de droit d'accès indirect	385	8,65 %	320	+20,30 %
Demandes d'information sur l'exercice des droits	238	5,35 %	146	+63,01 %
Demandes d'informations générales	242	5,43 %	201	+20,39 %
Demandes d'extraits du fichier des fichiers	155	3,48 %	170	- 8,82 %
Total	4 452	100 %	4 150	+7,27 %

Comparée à celle de l'année précédente, la nature des saisines reçues par la Commission traduit :
- une nette augmentation du nombre des demandes d'information sur l'exercice des droits (+63 *%}* et des demandes d'information générale (+20 %), qui manifeste une réelle prise de conscience des citoyens de l'importance des questions de libertés et de vie privée au regard de l'informatique ;
- une poursuite de l'augmentation des demandes de droit d'accès indirect, qui traduit là encore l'enracinement d'une culture « Informatique et libertés » dans l'opinion, même au regard de fichiers de police *(cf. infra).*

B. Les demandes de conseil

Les dix secteurs d'activité qui ont suscité en 1997 le nombre le plus important de demandes de conseil sont les suivants :
- prospection commerciale ;
- travail ;
- banque ;
- santé ;
- crédit ;
- télécommunications ;
- éducation ;
- fiscalité ;
- sécurité sociale ;
- immobilier.

L'objet le plus fréquent des demandes de conseil est par ordre d'importance décroissant le suivant :
— conditions de déclaration des traitements ;
- nature des obligations de sécurité des traitements et de confidentialité des informations ;
— modalités d'information des personnes concernant un traitement ;
— le droit d'accès aux informations d'un fichier.

C. Les plaintes

Les secteurs d'activité qui ont suscité en 1997 le nombre le plus important de plaintes sont les suivants :
- prospection commerciale ;
- banque ;
- travail ;
- crédit ;
- télécommunications (notamment l'identification de l'appelant) ;
- assurance ;
- fiscalité ;
- éducation nationale ;
- sécurité sociale.

L'objet le plus fréquent des plaintes est, par ordre décroissant, le suivant :
- exercice du droit d'accès indirect ;
- exercice du droit d'opposition ;
- exercice du droit d'accès direct ;
- pertinence des données ;
- collecte frauduleuse, déloyale ou illicite d'informations ;
- communication d'informations à des tiers non autorisés ;
- exercice du droit d'accès à des informations médicales ;
- absence d'information des personnes au moment de la collecte des données.

D. Les demandes de droit d'accès indirect

En application des articles 39 et 45 de la loi du 6 janvier 1978, les investigations nécessaires à l'instruction des demandes d'accès aux traitements automatisés et aux fichiers intéressant la sûreté de l'Etat, la défense et la sécurité publique sont effectuées par ceux des membres de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes.

1) LES DEMANDES RE!UES EN 1997

On constate par rapport à l'année précédente, une progression de 20 % du nombre de demandes de droit d'accès indirect à ces traitements et fichiers.

Bien que les chiffres enregistrés demeurent inférieurs aux deux années qui ont suivi la publication, en 1991, des décrets relatifs aux fichiers gérés par les services des Renseignements généraux du ministère de l'Intérieur, l'augmentation sensible du nombre de saisines enregistrée en 1996 (+31 *%)* se confirme en 1997 (+20 %).

Cette évolution paraît bien confirmer une meilleure connaissance du droit reconnu à chaque personne de demander que soit vérifiée la nature des informations éventuellement détenues sur son compte par les services de la police.

Les requérants saisissent généralement 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 titre de séjour du fait de l'inscription dans le système d'information Schengen

(cf. 17^{e} rapport, p. 445),
— à la suite d'une interpellation par les services de police.

	1989	**1990**	1991	1992	**1993**	**1994**	1995	**1996**	1997	Total
Requêtes	69	182	562	531	374	282	243	320	385	2 948
Evolution	-0,01 %	+ 164 %	+209 %	-5 %	- 29 %	- 25 %	- 14 %	+31%	+20 %	

Les 385 demandes reçues par la CNIL en 1997 correspondent à 652 vérifications, une même requête concernant souvent l'accès indirect à plusieurs traitements ou fichiers ; cela traduit une augmentation de 24 % des vérifications à effectuer par rapport à 1996.

2) LES DEMANDES TRAITEES EN 1997

Le nombre de vérifications effectuées au cours de l'année 1997 est de 639 et concerne des requêtes reçues en 1995, 1996 et en 1997. Ce chiffre aurait été plus élevé si dix-huit requérants n'avaient pas, en cours d'instruction de leur dossier, retiré leur demande ou omis de transmettre les éléments relatifs à leur identité précise.

Ministère de l'intérieur	**572**
- renseignements généraux (RG)	352
- police judiciaire (PJ)	72
- police urbaine (PU)	73
- direction de la surveillance du territoire (DST)	47
- système d'information schengen (SIS)	27
Douanes (FNID)	1
Ministère de la défense	67
- gendarmerie nationale (GEND)	31
- direction de la protection de la sécurité de la défense (DPSD)	15
- direction générale de la sécurité extérieure (DGSE)	16
- direction de la sûreté et de la protection du secret (DSPS)	5
Total	**639**

Il est important de noter que **572** de ces **639** vérifications ont eu lieu au ministère de l'Intérieur, soit 90 % du total et **67** au ministère de la Défense, soit 10 % du total.

Ce sont principalement les fichiers des Renseignements généraux qui sont visés dans les saisines. Ceci s'explique par le régime particulier de ces fichiers, qui ouvre des droits plus larges aux personnes *(cf. infra),* mais également par plusieurs raisons ponctuelles :

- la parution dans la presse de nombreux articles relatifs aux services des Renseignements généraux et la publication de livres consacrés à ce sujet, ainsi que des émissions de radio et de télévision qui, évoquant ces fichiers de police, ont fait connaître à un large public la possibilité offerte par la loi du 6 janvier 1978 aux citoyens de recourir au droit d'accès indirect ;
- les événement relatifs aux sectes évoqués dans la presse et la référence dans le rapport officiel sur les sectes en France à un recensement établi par les

Renseignements généraux ont sensibilisé des personnes qui craignaient d'être fichées à ce titre ;
- enfin, à titre anecdotique, plusieurs demandes de droit d'accès indirect ont pour origine un travail demandé à des étudiants d'un cours de libertés publiques (« Avez-vous cherché à exercer via la CNIL un accès indirect à un fichier ? »).

Pour ce qui concerne les traitements et fichiers relevant exclusivement de l'article 39 de la loi du 6 janvier 1978, soit l'ensemble de ceux mis en œuvre par les services des ministères de l'Intérieur et de la Défense à l'exception des Renseignements généraux, le résultat des 287 vérifications effectuées est le suivant :

Service	PJ	PU	DST	SIS	GEND	Autres : FNID DPSD DGSE DSPS	Total
Pas de fiche	24	46	39	7	8	24	148
Fiche sans suppression d'informations	39	26	7	12	19	10	113
Suppression totale ou partielle d'informations	9	1	1	8	4	3	26
Total	72	73	47	27	31	37	287

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

En fait, trois situations peuvent se présenter :
1) si les Renseignements généraux ne détiennent aucune information nominative concernant un requérant, la CNIL en informe ce dernier, en accord avec le ministre de l'Intérieur ;
2) si les Renseignements généraux détiennent des informations nominatives concernant un requérant, celles qui ne mettent pas en cause la sûreté de l'État, la défense et la sécurité publique lui sont communiquées, en accord avec le ministre de l'Intérieur. Dans l'hypothèse d'une communication totale ou partielle d'un dossier, le requérant a la possibilité de rédiger une note d'observations ; la Commission transmet au ministre de l'Intérieur cette note d'observations qui est insérée dans le dossier détenu par les services des RG ;
3) si la communication de tout ou partie des informations peut nuire à la sûreté de l'État, la défense et la sécurité publique, le magistrat membre de la CNIL procède à l'examen du dossier et, s'il y a lieu, exerce le droit de rectification ou d'effacement des données inexactes ou des données dont la collecte est

interdite par la loi. Le président de la CNIL adresse ensuite au requérant une lettre recommandée lui indiquant qu'il a été procédé aux vérifications conformément aux termes de l'article 39 de la loi du 6 janvier 1978. Cette lettre mentionne que la procédure administrative est close et indique les voies et délais de recours contentieux qui sont ouvertes au requérant.

Pour ce qui concerne les fichiers des Renseignements généraux, le résultat des 352 investigations menées en 1997 est le suivant :

• Pas de fiche au nom du requérant : 213
soit 60 % du total des vérifications effectuées aux RG.

• Existence d'une fiche : 139
soit 40 % du total des vérifications effectuées aux RG.

• Dossier jugé non communicable : *57*
soit 41 % de ceux qui avaient une fiche aux RG.

• Communication acceptée par le ministre de l'Intérieur : 82
soit 59 % de ceux qui avaient une fiche aux RG dont :
— communication totale du dossier : *75 ;*
— communication partielle du dossier : 7.

Il doit être relevé que, de même que les années précédentes, le ministre de l'Intérieur n'a refusé aucune des propositions de communication de dossier faites par les membres de la CNIL.

La procédure de communication des dossiers, initialement fixée par un protocole du 12 février 1992 arrêté avec le ministre de l'Intérieur, a fait l'objet d'une circulaire complémentaire du 2 juin 1993.

Depuis cette date, la procédure est la suivante :
- 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 1997 :
- 36 ont eu lieu au siège de la CNIL ;
- 46 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé.

À la suite de ces communications, seulement six requérants ont rédigé une note d'observations qui a été insérée dans le dossier des Renseignements généraux les concernant.

3) EVOLUTION DES INVESTIGATIONS EFFECTUEES AUPRÈS DES RENSEIGNEMENTS GÉNÉRAUX DEPUIS LE DÉCRET DU 14 OCTOBRE 1991

	1992	1993	1994	1995	1996	1997
Nombre de demandes traitées	766	320	273	197	252	352
Le requérant n'était pas fiché aux RG	421 *[55* %)	177 (55 %)	164 (60 %)	113 (57 *%)*	145 (58 %)	213 (60 %)
Le requérant était fiché aux RG	345 (45 %)	143 (45 %)	109 (40 %)	84 (43 %)	107 (42 %)	139 (40 %)
Le dossier a été jugé non communicable (%sur le nombre de requérants fichés)	90 (26 %)	50 (35 %)	44 (40 %)	25 (30 %)	33 (31 %)	57 (41 %)
La communication demandée a été refusée par le ministre de l'Intérieur (% sur le nombre de requérants fichés)	13(4 %)	0	0	0	0	0
La communication a été acceptée par le ministre de l'Intérieur (% sur le nombre de requérants fichés)	242 (70 %)	93 (65 %)	65 (60 %)	59 (70 %)	74 (69 %)	82 (59 %)
- dont communication totale du dossier - communication partielle du dossier	200 42	75 18	**27** 38	44 15	63 11	*75* *7*

4) RÉSULTATS DES INVESTIGATIONS CONCERNANT LE SYSTÈME D'INFORMATION SCHENGEN

La CNIL a reçu, au 31 décembre 1997, soixante-trois demandes de droit d'accès aux fichiers du système d'information Schengen.

Ces soixante-trois requérants étaient de vingt-huit nationalités différentes :

- France : dix ;
- Europe (moins la France) : vingt et un
- Afrique : vingt-cinq ;
- Amérique : un ;
- Asie : six.

Parmi ces soixante-trois saisines :

- quinze personnes n'étaient pas fichées ;
- quatorze personnes étaient signalées par la France ;
- vingt-neuf personnes étaient signalées par l'Allemagne ;
- une personne était signalée par la Belgique ;
- une personne était signalée par les Pays-Bas ;
- trois n'ont pas encore fait l'objet d'investigations

Parmi ces soixante-trois demandes de droit d'accès :

- L'instruction de cinquante-huit demandes est terminée en ce qui concerne la CNIL :

- quinze personnes n'avaient pas de fiche ;
- vingt-cinq personnes avaient une fiche qui devait être maintenue, dont six pour des problèmes d'alias ;
- deux fiches ont été supprimées par le bureau Sirène Français ;
- seize fiches ont été supprimées par le bureau Sirène Allemand.

- Cinq demandes sont en cours d'instruction :

- trois en attente d'investigations au N-SIS ;
- deux en attente des résultats d'investigations dans d'autres fichiers de police français.

IV. LA COMMUNICATION ET L'INFORMATION

A. Le vingtième anniversaire de la loi du 6 janvier 1978

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a eu vingt ans. Cette date anniversaire a été marquée par trois événements :

1) une remise de prix « informatique et libertés » ;
2) la publication d'un ouvrage intitulé *Les libertés et l'informatique -20 délibéra tions commentées ;*
3) l'ouverture du site Internet de la CNIL.

1) UNE REMISE DE PRIX « INFORMATIQUE ET LIBERTÉS »

La CNIL a réuni, salle Pleyel, ficheurs et fichés : administrations, entreprises, associations de défense des Droits de l'homme, syndicats, universitaires, chercheurs....

Placée sous le haut patronage du Président de la République, la soirée anniversaire s'est déroulée en présence de membres du Gouvernement et de nombreuses personnalités parmi lesquelles les présidents de plusieurs autorités étrangères de protection des données.

Au cours de cette manifestation, des prix « informatique et libertés » ont été décernés à des personnes ou des organismes qui, depuis vingt ans, ont agi pour la protection des données. Ainsi, ont été symboliquement récompensés : — Monsieur Bernard Siouffi, délégué général du syndicat des entreprises de vente par correspondance et à distance et de l'union française du marketing direct pour sa contribution à l'élaboration d'un code de déontologie en matière de protection des données à caractère personnel ;

- le lycée Charles de Gaulle à Muret (Haute-Garonne), pour la création d'une Commission locale de l'informatique et des libertés (CLIL) dans le cadre du système « Lycéoduc » ;
- Monsieur le professeur Gérard Lyon-Caen, pour ses travaux sur les libertés publiques et l'emploi et sa contribution à la protection des données dans le monde du travail ;
- l'Union fédérale des consommateurs — Que Choisir, pour ses enquêtes et ses actions d'information sur les droits des consommateurs face aux fichiers ;
- l'association AIDES, pour sa constante vigilance dans le domaine de la protection des données de santé ;
- la Poste, pour la conception d'un porte-monnaie électronique anonyme et son action en faveur de sa promotion.

2) LA PUBLICATION D'UN OUVRAGE INTITULÉ LES LIBERTÉS ET L'INFORMATIQUE — 20 DÉLIBÉRATIONS COMMENTÉES

Du premier avis défavorable rendu par la CNIL en 1981 à propos d'un système de sélection automatique des nouveau-nés devant faire l'objet d'un suivi médico-social au basculement de l'annuaire des abonnés au téléphone sur Internet, en passant par la mise en place du système informatisé Schengen, la segmentation comportementale bancaire ou les mégabases de données de consommation, c'est un florilège de décisions particulièrement significatives qui ont été commentées dans un recueil publié à La Documentation française. Cet ouvrage témoigne de l'importance de l'activité de la Commission et de la diversité de ses méthodes dans l'application de la loi.

3) L'OUVERTURE DU SITE INTERNET DE LA CNIL

Ouvert le 6 janvier 1998, le site de la CNIL est, sous de nombreux aspects, comparable à d'autres sites institutionnels. En effet, il contient de nombreuses informations concernant la loi « informatique et libertés », les droits des personnes, les obligations des détenteurs de fichiers ou encore les modalités de déclaration des traitements informatiques. De même, chaque internaute peut consulter et télécharger plus de soixante-dix textes officiels et des dossiers thématiques.

Mais ce site fait apparaître pour la première fois aux internautes comment ils laissent, à leur insu, des traces sur Internet *[cf. infra* dans ce chapitre et annexe 6).

B. La sensibilisation à la loi « Informatique et Libertés »

Dans le cadre de sa mission de formation et d'information en matière de protection des données personnelles et de la vie privée, la CNIL organise ou participe à de nombreuses rencontres destinées à sensibiliser les différents

acteurs, responsables de fichiers ou personnes fichées, aux obligations et aux droits des uns et des autres.

À cet égard, il convient de saluer l'initiative de l'UNEDIC, gros utilisateur de données personnelles, pour organiser à son siège, du 3 au 5 novembre 1997, une exposition sur la CNIL et ses missions.

De même, la CNIL a rencontré de nombreuses organisations syndicales les 22 et 29 avril 1997, afin de les sensibiliser à la protection des données personnelles dans le monde du travail ; à cette occasion, la Commission a diffusé un document rassemblant des fiches pratiques destinées à fournir des réponses aux problèmes qui peuvent se poser dans les entreprises (badges, autocommutateurs, vidéosurveillance...).

Enfin, dans le souci d'améliorer l'information des utilisateurs de l'informatique, la CNIL a élaboré en 1997 plusieurs guides pratiques qui sont disponibles gratuitement sur simple demande au siège de la CNIL ou consultables sur son site Internet.

Ainsi, la CNIL a élaboré un guide *Collectivités locales, informatique et libertés,* qui rassemble les conseils, avis et recommandations de la Commission dans ce domaine. Ce recueil, qui a notamment été présenté au salon des collectivités locales, est à la disposition de tous — élus, services municipaux, administrés — afin d'étendre la connaissance des droits et devoirs au regard de la protection des données personnelles. Ce guide comprend deux parties : la première est consacrée aux renseignements pratiques sur les formalités à accomplir auprès de la CNIL ; la seconde se présente sous la forme de fiches thématiques ; enfin, des annexes rassemblent des documents officiels tels que le texte de la loi du 6 janvier 1978 ou les normes simplifiées applicables aux collectivités locales.

La Commission a également conçu un guide pratique à l'attention des professions libérales de santé, intitulé *Santé, Informatique et libertés.* Il vise à permettre aux professionnels d'informatiser leurs cabinets dans le respect de la loi du 6 janvier 1978. Ainsi, la CNIL fournit des renseignements pratiques sur les précautions à prendre à cette occasion (matériel, formalités administratives, sécurité), des fiches thématiques rappelant les grands enjeux dans ce secteur (cartes santé « SÉSAM-VITALE », utilisation du numéro de sécurité sociale, droit d'accès des patients...). Ce document a notamment été distribué au salon du Médec qui s'est tenu à Paris du 25 au 28 mars 1998.

De plus, afin de simplifier les procédures de déclaration, il est désormais proposé aux professionnels de santé de ne remplir, en annexe au formulaire habituel, qu'un questionnaire pré-rédigé comportant l'ensemble des renseignements requis. Une démarche similaire a également été conduite auprès des notaires afin de faciliter la déclaration de leurs fichiers de clientèle.

Enfin, présenté sous le titre Je *monte mon site sur Internet,* la Commission a élaboré un document qui décrit les précautions à prendre lors de la création d'un site Internet et les formalités à accomplir auprès de la CNIL à cette occasion.

C. La participation à des colloques, salons, débats et conférences

Afin de se tenir informée des progrès réalisés dans le domaine des techniques informatiques, la CNIL a participé au cours de l'année 1997, à de nombreux colloques, salons, débats et conférences (Sécuricom, Imagina...). La Commission a été présente dans de nombreux séminaires destinés à réfléchir aux enjeux de l'Internet, que ce soit dans le domaine de la santé, du travail, de la sécurité, des transports ou de l'administration.

Une délégation de la CNIL s'est rendue à Dallas et à Tulsa du 1er au 3 décembre 1997, afin de participer à une réflexion sur les systèmes internationaux de réservation aérienne.

D. L'accueil de visiteurs étrangers et de stagiaires

La CNIL a reçu des délégations de plusieurs pays, notamment du Canada, du Cambodge et du Japon.

Malgré ses faibles possibilités d'accueil tenant à la charge de travail qui incombe à ses services, la Commission a reçu trois stagiaires en 1997 : Melle [redacted], élève en classe de 3e, dans le cadre d'un stage découverte de quatre jours, M. [redacted] et Melle [redacted], étudiants en troisième cycle de droit.

E. L'information du public

1) LE SITE INTERNET DE LA CNIL

La CNIL a ouvert ce site Internet le 6 janvier 1978, à l'occasion du vingtième anniversaire de la loi « Informatique et Libertés ». Ce site est accessible à l'adresse http://www cnil.fr.

La CNIL a entièrement conçu son site, de l'architecture à la rédaction de son contenu ; il est hébergé chez un prestataire mais la CNIL l'administre de façon autonome. Dans la phase précédant l'ouverture du site, la Commission a fait appel à deux prestataires, l'un pour créer la charte graphique et navigation-nelle et assurer l'intégration HTML ; l'autre pour prendre en charge certains développements techniques et l'hébergement.

Depuis son ouverture, le site de la CNIL a rencontré un vif succès dans le public et un large écho dans la presse et les médias ; il est souvent recensé parmi les meilleurs sites de l'Administration.

Le contenu du site

Les internautes trouvent sur le site web de la CNIL de nombreuses informations sur la protection des données personnelles, la loi « Informatique et Libertés » et la CNIL :

- la rubrique « **Actualités** » contient les communiqués de presse et d'autres documents d'information ponctuelle ;
- la rubrique « **La CNIL** » présente l'organisation de la Commission et ses missions ;
- la rubrique « **Textes** » rassemble plus de soixante-dix textes législatifs, réglementaires, internationaux, ainsi que les recommandations et les normes simplifiées émises par la CNIL ;
- la rubrique « **Droits et obligations** » décrit les modalités d'exercice des droits et de respect des obligations ;
- la rubrique « **Comment déclarer ?** » constitue une aide en ligne pour accomplir les formalités préalables ;
- la rubrique « **Dossiers thématiques** » contient notamment des dossiers intitu lés « La protection des données personnelles et Internet », « Informatique et libertés dans le monde », ou encore « Collectivités locales, informatique et libertés » ;
- la rubrique « **Publications** » donne les références des publications de la CNIL ;
- la rubrique « **Liens** » dirige l'internaute vers les sites des commissions étrangères et quelques sites français ;
- la rubrique « **Informations pratiques** » explique notamment le fonction nement du centre de documentation et les modalités de radiation des fichiers commerciaux.

De plus, le site propose une rubrique originale intitulée « **Vos traces** », qui permet à chaque internaute de découvrir comment il peut être « pisté » sur Internet. En effet, l'intégralité du parcours de l'internaute peut lui être restitué en direct, démonstration interactive que les déplacements sur le réseau sont repé-rables. Le site de la CNIL dévoile ainsi les procédés de « traçage »des personnes qui sont généralement utilisés pour repérer l'activité des internautes et détaille la technique et ses enjeux. Cette rubrique revêt un intérêt pédagogique évident en ce qui concerne les problèmes de confidentialité des données personnelles qui peuvent se poser sur Internet (cette rubrique est reproduite en annexe 6).

Le site de la CNIL en chiffres

Statistiques de fréquentation sur le 1er trimestre 1998 :

Mois	Nombre de requêtes faites au site (*Hits)*	Réponses envoyées par le site en mégaoctets	Nombre de pages HTML chargées	Pages les plus consultées
Janvier	906 515	4 096,779	353 883	Accueil : 23 404 Traces : 22 621
Février	535 429	2 547,202	212 191	Accueil : 14 905 Traces : 12 549
Mars	723 719	3 288,594	286 066	Accueil : 20 246 Traces : 17 443

En moyenne, la fréquentation hebdomadaire se décompose en 95 500 requêtes de pages HTML par jour ouvrés de la semaine et 12 960 pour le week-end.

Au cours de la première semaine qui a suivi l'ouverture du site, une fréquentation de 5 988 adresses IP uniques a été constatée.

Dans une boîte aux lettres (« vosreactionscnil.fr »), destinée à recevoir les réactions des internautes sur le contenu de la rubrique « Vos traces », la CNIL a été destinataire, sur les quatre premiers mois de l'année 1998, de près de 650 messages, dont :
- 90 % de réactions positives, assorties dans 30 % des cas de questions ou de commentaires motivés ;
- 3 % de messages négatifs ;
- 7 % de remarques neutres.

2) LE « 3615 » CNIL

Le service télématique d'information de la Commission — « 3615 CNIL »
- créé en 1990 et accessible par reroutage depuis « MGS » et « 3615 Vosdroits », a enregistré près de 13 500 appels en 1997 pour un total d'environ 1 300 heures de connexion.

Le « 3615 CNIL » comporte les rubriques suivantes :
- textes ;
- membres et services ;
- missions de la CNIL ;
- vos droits ;
- obligations des détenteurs de fichiers ;
- comment déclarer vos traitements ;
- recevoir des formulaires ;
- renseignements pratiques ;
- publications ;
- flash actualités.

3) LES CONFERENCES DE PRESSE

La CNIL a tenu une conférence de presse, le 7 juillet 1997, à l'occasion de la publication de son 17e rapport d'activité.

Par ailleurs, le 1er rapport d'activité de l'autorité de contrôle commune de Schengen (ACC) a été présenté par le président de l'ACC, M. Alex Türk, membre de la CNIL, le 18 juin 1997, lors d'une conférence de presse qui s'est tenue au siège de la Commission (cf. 17e rapport, p. 445).

Chapitre 2

LA LOI DU 6 JANVIER 1978 :

TEXTES, DOCTRINE,

JURISPRUDENCE

I. LES TEXTES

A. Les travaux relatifs à la transposition de la directive européenne du 24 octobre 1995

C'est lors de son discours à Hourtin sur l'entrée de la France dans la société de l'information, prononcé le 25 août 1997, que le Premier ministre a annoncé son intention de confier à Monsieur Guy Braibant, président honoraire de section au Conseil d'État, une mission d'étude préparatoire à l'élaboration d'un avant-projet de loi de transposition de la directive européenne du 24 octobre 1995.

LE RAPPORT BRAIBANT

Désigné par une lettre de mission du Premier ministre, le 12 septembre 1997, Monsieur Braibant a remis son rapport le 26 février 1998 après avoir procédé à plus de deux cent auditions, entendu chacun des membres de la CNIL et eu l'occasion de procéder à un large échange de vues, le 17 février 1998, avec la Commission réunie en séance plénière.

Ce rapport est publié à La Documentation française sous le titre *Données personnelles et société de l'information. Il* est également disponible sur le site Internet du Premier ministre.

Invitée par le Premier ministre à se prononcer sur ce rapport, la Commission a délibéré lors de sa séance du 31 mars 1998 et a adressé ses observations au Premier ministre le 3 avril 1998. Le 28 avril 1998, le président Jacques Fauvet, le vice-président délégué Michel Benoist et le vice-président

Raymond Forni ont été reçus par Monsieur le directeur du cabinet du Premier ministre pour lui faire part du sentiment de la Commission sur les grandes orientations de la réforme.

La CNIL a souhaité exprimer sa satisfaction sur les conditions dans lesquelles elle était associée au travail de réforme que commande la transposition. Elle a en outre été sensible à l'engagement du Premier ministre de la consulter sur l'avant projet de loi qui constituera la deuxième étape de la réforme avant que ne s'engage le débat au Parlement.

LA CNIL FAIT DES PROPOSITIONS POUR UNE RÉFORME

La transposition en droit français de la directive européenne touche une matière relevant pour une part essentielle des libertés publiques et ne saurait constituer un exercice de pure technique juridique. La CNIL a fait diverses propositions qui renforcent, rejoignent ou complètent celles qui ont été faites par la mission Braibant. Les plus importantes sont les suivantes":

1) Simplifier ou supprimer les procédures déclaratives pour les traitements d'usage courant

La directive y invite en préconisant un simple système de notification des traitements appelé à se substituer, au moins partiellement, à l'actuel système déclaratif (dossier de demande d'avis ou dossier de déclaration ordinaire).

La CNIL pense, avec le président Braibant, qu'on peut aller plus loin en exonérant purement et simplement de toute notification à l'autorité de contrôle les traitements d'usage courant, le soin revenant à celle-ci d'élaborer à cet effet des normes d'exonération et de les mettre en œuvre. L'expérience acquise par la CNIL qui a, en vingt ans, édicté trente-neuf normes simplifiées destinées à alléger les formalités de déclaration pour les traitements les plus courants témoigne de l'efficacité de cette procédure : plus de 80 % des traitements déclarés dans une année le sont désormais selon une procédure simplifiée. Ces normes simplifiées pourraient constituer une solide base de départ permettant à la future autorité de contrôle d'édicter, si la future loi le lui permettait, des normes d'exonération.

2) Faire bénéficier, en tout ou partie, les personnes morales des dispositions protectrices de la loi du 6 janvier 1978

Les fichiers d'entreprises se multiplient qui concernent tout à la fois des personnes morales et des personnes physiques (dirigeants, associés). Ces fichiers et les conditions de leur consultation peuvent avoir une grande incidence non seulement sur la vie économique de l'entreprise mais aussi sur la réputation professionnelle ou personnelle de leurs dirigeants.

Déjà le législateur de 1978 avait envisagé de faire bénéficier les personnes morales de la protection de la loi, avant d'y renoncer. Le moment paraît venu de le faire.

3) Inclure les données génétiques dans les catégories de données sensibles

Le caractère potentiellement prédictif des données génétiques leur confère incontestablement une sensibilité particulière, leur exploitation pouvant avoir de graves répercussions sur la vie privée, sociale ou professionnelle des personnes. Le président Braibant propose d'inclure les données génétiques dans les catégories de données dites « sensibles ». Cette proposition, rejoint le vœu de la CNIL qui, dans une recommandation du 19 février 1985, avait déjà préconisé que des garanties particulières soient prises en matière de fichiers génétiques à des fins de recherche médicale. •

4) Assurer une plus grande transparence en renforçant le droit d'accès

La loi du 6 janvier 1978 a institué une procédure particulière en matière de droit d'accès aux fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique. Dans ce cas, le droit d'accès s'exerce par l'Intermédiaire d'un membre de la Commission appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation et à la Cour des comptes, seuls habilités par la loi à mener des investigations dans ces fichiers. À l'issue de la procédure de vérification, l'information donnée au requérant se limite au seul fait que « les vérifications ont été faites ». Cette formulation n'est pas toujours satisfaisante et, dans un grand nombre de cas, les personnes concernées pourraient être informées qu'elles ne sont pas fichées ou qu'elles ne le sont plus à l'issue des vérifications, sans qu'il en résulte une atteinte à un intérêt supérieur de l'État. Dans d'autres cas, l'information pourrait être communiquée à l'intéressé.

Le dispositif particulier prévu par le décret du 14 octobre 1991 relatif aux Renseignements généraux a constitué une avancée notable (cf. *supra 1re* partie, chapitre 1 et 12e rapport, p. 67). Il pourrait être étendu et prolongé. Ainsi, s'agissant du système Schengen, lorsque, à l'issue des vérifications, une fiche dont l'intéressé avait eu connaissance (à l'occasion d'un contrôle d'identité ou d'une formalité administrative) a été supprimée, il devrait pouvoir en être informé. S'agissant des fichiers de police judiciaire, dès lors que les renseignements concernent des procédures qui se sont achevées par une décision devenue définitive et qui a été régulièrement notifiée à l'intéressé, ce dernier pourrait en avoir directement connaissance, le cas échéant en s'adressant au procureur de la République.

Une plus grande transparence dans ce domaine paraît tout à la fois compatible avec la sauvegarde de l'intérêt public et de nature à renforcer les droits des personnes. Les conclusions du rapport Braibant y invitent le Gouvernement ; la CNIL soutient ces propositions.

Il est un autre domaine dans lequel les conditions d'exercice du droit d'accès ne paraissent pas à l'heure actuelle satisfaisantes : il s'agit du droit d'accès aux fichiers fiscaux. Le rapport Braibant propose d'appliquer aux

traitements qui ont pour but exclusif de lutter contre la fraude fiscale une dérogation au droit d'accès prévue par la directive européenne.

La loi du 6 janvier 1978 ne ménageant aucune dérogation au droit d'accès à l'égard des fichiers fiscaux, la réforme proposée devrait être de portée limitée, placée sous le contrôle de l'autorité de contrôle à laquelle reviendrait le soin de déterminer, à l'occasion d'un examen préalable, si tel traitement peut ou non bénéficier d'une dérogation de cette nature et prévoir un mécanisme du type de celui qui existe en matière de fichiers de sécurité publique. L'essentiel est que, dans tous les cas, les informations détenues par l'administration fiscale puissent être contrôlées, soit directement par la personne elle-même, soit par l'intermédiaire de l'autorité de contrôle.

Il pourrait incontestablement résulter d'un tel dispositif une amélioration des conditions dans lesquelles l'administration fiscale traite à l'heure actuelle les demandes de droit d'accès dont elle est saisie.

5) S'assurer des conditions de mise en œuvre des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, qu'ils soient d'origine publique ou privée

L'article 20 de la directive prévoit que les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées doivent faire l'objet d'un examen préalable. La simplification des procédures déclaratives (une simple notification de l'existence des traitements) ou l'exonération proposée par la CNIL de toute notification, ne saurait concerner ceux des traitements, peu nombreux mais « sensibles », dont l'existence ou les conditions de mise en oeuvre nécessitent une réflexion approfondie ou l'arbitrage d'un autorité indépendante.

La CNIL estime que tel doit être le cas pour les catégories de traitements suivantes :

- les traitements qui touchent à des matières dites « de souveraineté », exclues du champ d'application de la directive, et parmi lesquels figurent notamment les traitements de police judiciaire, de sécurité publique, de défense et de sûreté de l'État, les traitements touchant au droit pénal ou encore au contrôle de l'immigration et de la régularité du séjour des étrangers en France ;
- les traitements de données sensibles (origine ethnique, opinion politique, philosophique, religieuse, appartenance syndicale, moeurs, données génétiques) ;
- les traitements dont le fonctionnement dérogerait aux principes protecteurs des personnes ; ainsi si certains traitements fiscaux devaient bénéficier d'une dérogation au droit d'accès, l'autorité de contrôle devrait-elle être saisie des conditions de leur mise en œuvre ;
- les traitements utilisant le numéro d'identification au répertoire (NIR ou numéro de sécurité sociale) ou tout autre identifiant de portée générale ;
- les interconnexions entre fichiers à finalité distincte ;

- les traitements pouvant avoir pour effet d'exclure les personnes d'un droit, d'une prestation ou d'un contrat, tels les fichiers communs d'incidents de paiement, d'impayés locatifs, de « crédit scoring » ;
- les enquêtes statistiques revêtant un caractère obligatoire, tel le recensement général de la population ;
- les traitements concernant la totalité de la population ou une partie largement majoritaire de la population, tels les principaux traitements de sécurité sociale, d'EDF, de France Télécom etc. ;
- les traitements recourant ou nécessitant des transferts internationaux de données hors des frontières européennes ;
- les traitements reposant sur une technologie nouvelle ou sur l'usage nouveau d'une technologie plus ancienne.

C'est sur ce point sans doute que les propositions de la CNIL s'éloignent le plus de celles du rapport Braibant.

La CNIL estime cependant que le nombre de traitements relevant de ces catégories est très faible par rapport au nombre de traitements existant en France, la liste proposée correspondant au demeurant à ceux des traitements qui, compte tenu de leur portée, de leur importance ou de leur impact sur l'opinion, font l'objet d'un examen en séance plénière. Les discussions qu'ils suscitent, les aménagements que l'instruction des dossiers permet d'apporter ou les réserves émises par la Commission sur les conditions de leur fonctionnement, attestent que leur examen préalable par une autorité indépendante constitue une garantie fondamentale.

L'avis rendu par l'autorité de contrôle à l'occasion de cet examen préalable devrait évidemment pouvoir être contesté par le « déclarant » devant la juridiction administrative.

Enfin, dans un souci de souplesse, la faculté devrait être reconnue à l'autorité de contrôle de pouvoir élaborer des normes simplifiées destinées à alléger les procédures à accomplir devant elle dès lors que les caractéristiques d'un traitement en principe soumis à son examen préalable, respecteraient le dispositif de ces normes. Un tel dispositif serait particulièrement adapté en matière de « technologies nouvelles ». Ainsi, lorsqu'une technologie aurait perdu le caractère de nouveauté qui aurait justifié un examen préalable avant sa mise en œuvre, l'autorité de contrôle pourrait adopter une norme simplifiée destinée à alléger les formalités.

6) Renforcer les pouvoirs de contrôle a posteriori et garantir la sécurité juridique des responsables de traitements en reconnaissant à la future autorité de contrôle le pouvoir de fixer des normes pour la mise en œuvre de la loi

Le renforcement effectif des pouvoirs de contrôle a *posteriori* et la reconnaissance d'un véritable pouvoir de sanction administrative constituent un aspect majeur de la réforme. Compte tenu de l'exonération ou de l'allégement

des procédures de contrôle a *priori,* ces moyens juridiques sont indispensables pour que soit maintenu un haut niveau de protection des personnes concernées. De réels pouvoirs d'investigation doivent pouvoir être reconnus aux membres et agents de la future autorité de contrôle et tout particulièrement celui de procéder par contrôles inopinés, seuls de nature à éviter la dissimulation des preuves. Sur ce point, et pour l'essentiel, la CNIL soutient les propositions faites par le rapport Braibant.

Cependant, au-delà du renforcement des pouvoirs d'intervention a *posteriori,* la CNIL estime que l'autorité de contrôle doit disposer, dans certaines conditions, du pouvoir de fixer certaines règles pour la mise en oeuvre de la loi. Passer d'un contrôle a *priori* à un contrôle a *posteriori* pourrait emporter de nombreux inconvénients. C'est pourquoi la Commission estime que la future autorité de contrôle devrait pouvoir faire des recommandations juridiquement obligatoires, s'agissant tout particulièrement des mesures de sécurité des systèmes, des modalités d'information des personnes concernées, de la durée de conservation des informations et des catégories d'informations pouvant être collectées et traitées au regard des finalités du traitement.

Une disposition de cette nature permettrait aux opérateurs de disposer d'une règle claire et sûre. Elle n'aurait aucun caractère « répressif » et permettrait d'éviter la multiplication des missions ponctuelles de contrôle *a posteriori* ayant le même objet. Elle présenterait une grande souplesse dans la mesure où ces recommandations valant normes d'application pourraient très rapidement être adaptées aux évolutions technologiques, modifiées, assouplies.

Enfin, la réforme de la loi posera sans aucun doute le problème de la nature et des moyens de la future autorité de contrôle.

Le renforcement des moyens de la future autorité et tout particulièrement de ses personnels à haute compétence technique est une absolue nécessité, sauf à risquer un abaissement du niveau de protection des données en France.

S'agissant de la nature de la future autorité, que le président Braibant désigne sous le sigle de « CNIL 2 », le principe, retenu par le législateur de 1978, d'une autorité collégiale composée de représentants des assemblées parlementaires, de hauts magistrats et de personnes qualifiées pour leurs connaissances des applications de l'informatique, parait essentiel pour garantir l'indépendance de l'institution, la richesse de ses débats au service des droits fondamentaux de la personne et marquer la nature de ses missions. À cet égard, le défi que lance la mondialisation des échanges de données, tout particulièrement à l'heure d'Internet, ne doit conduire la France ni à renoncer à des principes qui ont su s'adapter à tous les sauts technologiques et qui constituent désormais le socle commun des pays européens, ni à transformer la future autorité de contrôle en un « bureau d'experts » qui paraîtrait éloigné des préoccupations des citoyens.

La transposition de la directive offre l'opportunité d'adapter la loi du 6 janvier 1978 au nouveau paysage informatique tout en conservant les acquis de la protection des données en France.

PREPARER L'AVENIR

La CNIL est déjà résolument tournée vers l'avenir : elle adapte ses pratiques, elle multiplie les contrôles sur place et renforce leur caractère technique ; parallèlement, elle poursuit sa politique d'allégement des procédures administratives de déclaration de fichiers ; enfin, elle renforce sa politique d'information des personnes sur leurs droits et leurs obligations, notamment par la diffusion de plusieurs guides thématiques « Informatique et Libertés » et l'ouverture d'un site Internet contenant de nombreux documents télédéchargea-bles (*cf. supra 1*re partie, chapitre 1).

B. L'avis de la CNIL sur l'avant-projet de loi tendant à harmoniser les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, du 17 juillet 1978 relative à la liberté d'accès aux documents administratifs et du 3 janvier 1979 sur les archives

Le ministre de la Fonction publique, de la Réforme de l'État et de la Décentralisation a sollicité les observations de la CNIL sur un avant-projet de loi relatif aux droits des citoyens dans leurs relations avec les administrations.

S'agissant de la compatibilité de la loi du 6 janvier 1978 avec la loi sur les archives du 3 janvier 1979, une contradiction doit être levée. En effet, la loi « Informatique et Libertés » prévoit que la durée de conservation des informations enregistrées dans un traitement automatisé doit être limitée à ce que justifie la finalité du traitement ; la loi du 3 janvier 1979 pose quant à elle le principe de l'imprescriptibilité des archives, et tout particulièrement des documents administratifs, sans distinguer selon qu'ils sont conservés sur support papier ou sur support informatique.

L'avant-projet de loi soumis à la CNIL s'efforce de résoudre cette contradiction, tout en tenant compte des dispositions de la directive européenne du 24 octobre 1995. En effet, cette directive prévoit qu'au-delà de la durée justifiée par les finalités d'un traitement informatique, les informations peuvent être conservées sous une forme nominative en vue de leur traitement à des fins historiques, statistiques ou scientifiques.

L'avant-projet de loi prévoit que la conservation des informations à ces fins doit s'opérer alors dans des conditions prévues par la loi du 3 janvier 1979, c'est-à-dire notamment sans consultation possible par un tiers pendant un délai qui est en principe d'au moins trois ans. Cette conservation ne nécessitera plus d'autorisation de la CNIL. En revanche, ce texte prévoit que ces informations conservées pourront faire l'objet d'un traitement à des fins autres qu'historiques mais à la double condition que ce traitement soit opéré dans l'intérêt des personnes concernées et avec l'autorisation de la Commission. En outre, lorsque le traitement des informations archivées concernera des données sensibles, la

procédure prévue par l'article 31 de la loi du 6 janvier 1978 (décret en Conseil d'État pris après avis conforme de la CNIL) devra s'appliquer.

S'agissant de l'articulation entre la loi du 6 janvier 1978 et la loi du 17 juillet 1978 relatives notamment à la communication des documents administratifs, le projet de loi proposé tend à mettre fin à l'anomalie résultant de ce que certaines informations étaient communicables en vertu de la loi du 17 juillet 1978 si elles figuraient dans des documents sur support papier, mais ne l'étaient pas, en vertu de la loi du 6 janvier 1978, si elles faisaient l'objet d'un traitement informatique. Le 16e rapport d'activité de la Commission avait largement abordé ce problème en souhaitant une harmonisation des deux lois (cf. 16e rapport, p. 25).

L'avant-projet de la loi qui a été soumis à la CNIL reprend sur ce point les suggestions faites à l'époque par la Commission. Ainsi, dès lors qu'un document, quel que soit son support, sera communicable en vertu de la loi du 17 juillet 1978, l'administration sollicitée ne pourra pas invoquer la loi du 6 janvier 1978 pour faire obstacle à sa communication. En outre, la loi du 17 juillet 1978 serait modifiée afin d'élargir la notion de documents administratifs. Ainsi, les documents susceptibles d'être communiqués pourraient non seulement être « des documents existant sur support informatique » mais aussi les « documents pouvant être obtenus par un traitement automatisé simple », ce qui renforce la transparence administrative.

Sur l'ensemble de ces points, la CNIL a approuvé les termes du projet de loi.

II. LA DOCTRINE DE LA CNIL

A. L'application de l'article 31 de la loi du 6 janvier 1978 : la spoliation des personnes considérées comme juives par les autorités de Vichy ou les forces d'occupation

1) LE FICHIER DE LA VILLE DE PARIS

La mise en œuvre d'une nouvelle politique de gestion du domaine privé de la ville de Paris (environ 1 300 logements), qui doit conduire, d'une part au transfert aux bailleurs sociaux des logements remplissant une vocation sociale et, d'autre part, à la vente des logements ne répondant pas à ce critère social, a soulevé la douloureuse question des biens immobiliers dont les propriétaires considérés comme juifs par les autorités de Vichy auraient été spoliés pendant la période de l'occupation, avant de devenir la propriété de la ville de Paris.

Le Conseil du patrimoine privé, organisme consultatif indépendant mis en place pour étudier toutes les questions touchant la gestion domaniale privée de la ville, a donc été chargé d'identifier au sein du domaine privé de la ville de Paris, les immeubles dont l'acquisition résulterait de la spoliation de propriétaires victimes des actes discriminatoires du gouvernement de Vichy, puis de proposer à la municipalité toutes mesures adéquates.

Dans ce contexte, le Conseil du patrimoine privé a été conduit à constituer, pour le compte de la ville de Paris, un fichier dont la finalité est le recensement de l'identité des propriétaires considérés comme juifs par les autorités de Vichy ainsi que, le cas échéant, de leurs descendants ou ayants droit. Cette base de données comporte des informations relatives aux biens, aux modalités d'acquisition, à l'identité des propriétaires ou des locataires, à leur sort pendant la guerre, au bénéfice éventuel de mesures de réparation à la libération, aux héritiers ou ayants droit.

Ces informations proviennent, d'une part des actes de propriété établis par la mairie de Paris et, d'autre part, de divers documents d'archives relatives à cette période (Archives nationales, archives départementales de Paris, archives du Conseil d'État, du ministère des Finances, du Centre de documentation juive contemporaine...).

Saisie par la direction du logement et de l'habitat de la ville de Paris d'une demande d'avis concernant la mise en œuvre de ce fichier, la CNIL a constaté qu'il comporterait directement et indirectement, des données sensibles. L'article 31 de la loi du 6 janvier 1978 interdisant la collecte de telles données sauf accord exprès des intéressés, seul un décret en Conseil d'État pris sur proposition ou après avis de la CNIL, pouvait autoriser la collecte et l'enregistrement de telles données.

La CNIL a, en l'espèce, considéré que l'intérêt public, condition exigée par l'article 31 de la loi, justifiait pleinement la mise en oeuvre de ce traitement et donc la collecte de données sensibles. Elle a donc, pour la première fois et sans attendre d'être saisie d'un projet de décret, proposé et rédigé un projet de texte autorisant dans l'intérêt public la collecte et la conservation de telles informations sensibles. La Commission a été particulièrement attentive, dans la rédaction de ce texte, à ce que cette autorisation soit strictement limitée aux seuls biens immobiliers et à la seule ville demanderesse, afin d'empêcher que ne puissent se constituer, ici ou là et sans contrôle strict, des fichiers de personnes identifiées par la religion.

Par ailleurs, la CNIL a pris acte de ce que la mairie de Paris a souhaité verser une copie du fichier, une fois exploité, au Centre de documentation juive, dont l'objet est de réunir et de conserver la documentation se rapportant au génocide dont furent victimes les communautés juives des pays d'Europe sous la domination nazie. Un tel versement revêtait en effet un grand intérêt au regard de sa valeur de témoignage.

Au final, la CNIL a donné un avis favorable à la mise en oeuvre par la mairie de Paris d'un fichier informatique destiné à l'inventaire des biens immobiliers dont l'acquisition aurait pu résulter de spoliations de personnes qui ont pu être considérées comme juives par les autorités de Vichy, sous réserve que le Gouvernement adopte le projet de décret en Conseil d'État dont la Commission avait fait la proposition. Le décret dans sa forme définitive a été publié au *Journal officiel* du 14 septembre 1997.

Délibération n° 97-057 du 8 juillet 1997 relative à une proposition 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 Ville de Paris aux fins de recenser les biens immobiliers dont ont été spoliées des personnes considérées comme juives par les autorités de Vichy et d'identifier leurs ayants droit

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 31 et 45 ;

Après avoir entendu Madame Isabelle Jaulin et Monsieur Michel Bernard, commissaires en leur rapport et Madame Marie-Charlotte Pitrat, commissaire du Gouvernement en ses observations ;

Considérant que la loi du 6 janvier 1978, dans son article 31, 1er alinéa, dispose qu'aucune donnée nominative faisant apparaître directement ou indirectement les origines raciales ou les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou les moeurs des personnes, ne peut être mise ou conservée en mémoire informatique ; que cette disposition est applicable aux fichiers non automatisés en vertu du 1er alinéa de l'article 45 de la même loi ;

Considérant que le troisième alinéa de l'article 31 prévoit qu'il peut être fait exception à cette interdiction pour des motifs d'intérêt public, sur proposition ou avis conforme de la Commission par décret en Conseil d'État ;

Considérant que la CNIL a été saisie pour avis d'un traitement appelé à être mis en œuvre par la Ville de Paris destiné à permettre le recensement des biens immobiliers dont les personnes d'origine juive ont été spoliées par le régime de Vichy sous l'occupation et d'identifier leurs ayants droit ;

Considérant que parmi les informations nominatives faisant l'objet de ce traitement figurent le fait d'avoir été recensé comme juif par le régime de Vichy et le sort subi pendant la guerre ; que ces informations sont au nombre de celles qui, en application des dispositions de l'article 31 de la loi du 6 janvier 1978, ne peuvent être mises et conservées en mémoire à défaut du consentement exprès des intéressés que par dérogation accordée par décret en Conseil d'État pris sur proposition ou avis conforme de la Commission ;

Considérant que l'objectif poursuivi, qui consiste à faire toute la lumière sur l'ampleur des spoliations réalisées à l'encontre de personnes ayant fait l'objet de mesures discriminatoires du seul fait de leur appartenance à la communauté juive et à permettre leur identification et celle de leurs ayants droit, relève de l'intérêt public ;

Considérant dès lors qu'il convient de proposer au Gouvernement l'adoption d'un projet de décret autorisant la Ville de Paris à collecter et traiter des informations faisant apparaître directement ou indirectement l'origine juive des personnes propriétaires ou locataires de biens immobiliers qui ont fait

l'objet de spoliations par les autorités de Vichy aux seules fins de recenser ces biens et d'identifier les personnes concernées et leurs ayants droit ;

Propose au Gouvernement, conformément à l'article 31 alinéa 3 de la loi du 6 janvier 1978, d'adopter le projet de décret joint en annexe.

Délibération n° 97-058 du 8 juillet 1997 portant avis sur un projet d'arrêté du maire de Paris relatif à la création d'un traitement destiné à rechercher les conditions dans lesquelles des biens immobiliers auraient été acquis par la Ville de Paris, à la suite de spoliations de personnes considérées comme juives par le régime de Vichy

(Demande d'avis n° 520 306)

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 son article 31 ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

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

Vu l'arrêté du 28 février 1996 portant création du Conseil du patrimoine privé ; Vu le projet d'arrêté présenté par le maire de Paris ;

Après avoir entendu Madame Isabelle Jaulin et Monsieur Michel Bernard, commissaires, en leur rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Considérant que la Commission est saisie par la mairie de Paris, direction du logement et de l'habitat, d'une demande d'avis relative à un traitement dont Ta finalité est de rechercher les conditions dans lesquelles des biens immobiliers auraient été acquis par la Ville de Paris, à la suite de spoliations de personnes recensées comme juives par le régime de Vichy ;

Considérant que ce traitement doit être mis en oeuvre par le Conseil du patrimoine privé de la Ville de Paris dont l'une des missions est de recenser dans le domaine privé de la Ville de Paris les immeubles dont l'acquisition résulterait de la spoliation de propriétaires victimes des actes discriminatoires du gouvernement de Vichy et d'identifier leurs propriétaires et leurs descendants ou ayants droit ;

Considérant que les catégories d'informations appelées à figurer dans ce traitement informatique sont relatives à :

- l'adresse et la consistance du bien ;
- les modalités d'acquisition par l'ancien propriétaire et par la ville ainsi que le prix de la vente ;
- l'identité des propriétaires ou des locataires : nom, prénom, date et lieu de naissance, adresse, nationalité, recensé ou non comme juif par le régime de Vichy ;
- le sort subi par ces derniers pendant la guerre ;
- le bénéfice éventuel de mesures de réparation à la libération ;
- l'identité des héritiers ou ayants droit : nom, prénom, filiation, adresse.

Considérant que ces informations proviennent d'une part des actes de propriétés établis par la mairie de Paris et d'autre part, de documents recueillis auprès des détenteurs d'archives sur la période de l'Occupation (Archives nationales, départementales, des archives du ministère des Finances, du Centre de documentation juive contemporaine...) ;

Considérant que les informations se rapportant au recensement des personnes considérées comme juives par le régime de Vichy et au sort subi par ces personnes pendant la guerre sont de nature à faire apparaître l'origine religieuse de ces personnes ; que par délibération n° 97-057 en date de ce jour, la Commission a proposé, conformément aux dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978, un projet de décret autorisant la collecte et le traitement de telles données ;

Considérant que les destinataires des informations nominatives traitées seront exclusivement les membres du Conseil du patrimoine privé et des agents du service de la direction du logement et de l'habitat, de la direction de l'aménagement urbain et de la construction et de la direction des affaires juridiques de la Ville de Paris spécialement habilités à cet effet ;

Considérant qu'il est prévu que les informations ne soient pas conservées par la mairie de Paris au-delà du temps nécessaire à l'accomplissement de la mission du Conseil du patrimoine privé ; qu'à l'issue de cette période le traitement considéré, qui constitue une archive publique au sens des articles 1er et 3 de la loi du 3 janvier 1979, sera déposé aux archives départementales de Paris ;

Considérant en outre que la mairie de Paris prévoit de déposer une copie du fichier informatisé au Centre de documentation juive contemporaine ; que, s'il appartient aux autorités responsables de la conservation des archives de décider des conditions dans lesquelles celle-ci sera réalisée, il apparaît que la valeur de témoignage permanent des persécutions subies pendant l'Occupation par la communauté juive que revêt ce traitement est de nature à justifier l'intérêt de la démarche envisagée par la Ville de Paris ;

Considérant que les ayants droit des personnes concernées pourront, conformément à l'article 34 de la loi n° 78-17 du 6 janvier 1978, exercer leur droit d'accès auprès du Conseil du patrimoine privé ;

Émet un avis favorable sur le projet d'arrêté présenté par le maire de Paris sous réserve que, s'agissant des informations susceptibles de faire apparaître directement ou indirectement l'origine religieuse des personnes, le projet de décret, portant application des dispositions du 3e alinéa de l'article 31 de la loi du 6 janvier 1978 au fichier mis en œuvre par la Ville de Paris aux fins de recenser les biens immobiliers des personnes considérées comme juives par les autorités de Vichy et d'identifier leurs ayants droit, proposé par délibération de la Commission n° 97-057 en date de ce jour soit adopté et publié.

2) LA DEMANDE D'AVIS DU PREMIER MINISTRE

Les pouvoirs publics ont mis en place, dans le cadre d'une mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy et les forces d'occupation, un groupe de travail chargé d'évaluer l'ampleur des biens confisqués pendant la guerre.

Ce groupe de travail, créé auprès du Premier ministre par arrêté du 25 mars 1997, a reçu pour mission d'étudier les conditions dans lesquelles des biens immobiliers et mobiliers appartenant à des personnes considérées comme juives par les autorités de Vichy et les forces d'occupation et résidant en France ont été confisqués ou, d'une manière générale, acquis par fraude, violence ou dol, tant par l'occupant que par le Gouvernement de Vichy entre 1940 et 1 944. Cette mission a pour objet de rechercher la destination que ces biens ont reçue depuis la fin de la guerre, déterminer leur localisation et leur situation juridique actuelles, enfin d'établir un inventaire des biens accaparés sur le territoire français et qui sont encore détenus par les autorités publiques. Dans ce contexte, la mission d'étude a souhaité mettre en oeuvre un fichier destiné à recenser non seulement les biens immobiliers mais aussi les biens mobiliers (valeurs mobilières, œuvres d'art...) qui auraient pu être confisqués sur le territoire national par l'occupant ou le gouvernement de Vichy. La constitution d'un tel fichier posait, en termes de protection des données, une problématique semblable à celle du fichier précédemment décrit.

La constitution de ce fichier manifeste le rôle central tenu par la Caisse des dépôts et consignations, en tant que centre de consignation de toutes les sommes saisies en application de la législation de Vichy et décidées par le commissariat général aux questions juives. Rôle important aujourd'hui, dans la mesure où cet organisme pourrait détenir des fiches et des registres pouvant comporter les nom, adresse, le montant des sommes relatives aux spoliations et la trace des restitutions opérées à la libération. C'est la raison pour laquelle la Caisse des dépôts est chargée de la mise en œuvre du traitement informatique à partir de trois ordinateurs respectivement placés dans ses locaux, auprès des archives de France et à la préfecture de police. Concrètement, la constitution du fichier doit résulter du croisement d'informations détenues par divers ministères, par les Archives nationales qui possèdent notamment les dossiers du commissariat aux questions juives, par la Caisse des dépôts et consignations, la préfecture de police, le Centre de documentation juive contemporaine.

Les informations collectées sur les personnes spoliées sont les nom, prénom, adresse, profession, date et lieu de naissance, nationalité, nom et prénom des membres de la famille, nom et prénom des personnes qui se sont éventuellement déclarées comme ayants droit à la Libération et le sort de la personne et des membres de sa famille pendant et après la guerre. Les informations relatives aux biens dont les propriétaires ont été dépossédés, que ces biens aient été mis sous séquestre ou administrés par des tiers, portent sur les nom et qualité des dépositaires et administrateurs provisoires et sur les opérations qui ont été effectuées sur les biens par les dépositaires et administrateurs provisoires. Les informations sur les restitutions opérées après la guerre concernent l'identité des personnes ayant réclamé le bien et des personnes appelées à le restituer. Ainsi, le traitement devrait permettre d'évaluer le montant des biens concernés par une spoliation, de déterminer leur destination pendant l'occupation et leur éventuelle restitution après la Libération.

Le projet d'arrêté portant création du fichier de recensement de ces personnes a été présenté accompagné d'un projet de décret en Conseil d'État

visant à lever, pour des motifs d'intérêt public, l'interdiction de mettre en mémoire des données sensibles relevant de l'article 31 de la loi du 6 janvier 1978. Toutefois, dans le souci de limiter les informations sensibles appelées à figurer dans ce fichier hors du commun, la CNIL a souhaité que soient précisées celles des données sensibles visées par l'article 31 de la loi du 6 janvier 1978 dont la finalité du fichier justifierait qu'elles fussent recueillies. La CNIL a demandé qu'il soit précisé que la collecte des données sensibles ne visait que des personnes victimes de spoliation qui ont été considérées comme juives par les autorités de Vichy et les forces d'occupation. Les actes réglementaires relatifs à ce traitement ont été modifiés en conséquence puis publiés au *Journal officiel* du 25 décembre 1997.

Délibération n° 97-092 du 2 décembre 1997 relative à un projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 au fichier mis en œuvre par la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy

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 31 et 45 ;

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

Considérant que le Premier ministre a présenté à la Commission un projet de décret autorisant la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy et les personnes travaillant pour son compte et sous son contrôle à collecter et traiter des informations relevant du troisième alinéa de l'article 31 de la loi du 6 janvier 1978;

Considérant que la CNIL a parallèlement été saisie d'une demande d'avis relative à un traitement appelé à être mis en œuvre par la mission d'étude sur la spoliation durant l'Occupation des biens appartenant aux juifs résidant en France, instituée auprès du Premier ministre, et les personnes travaillant pour son compte et sous son contrôle, destiné à permettre l'évaluation de l'ampleur des spoliations subies par les personnes considérées comme juives par les autorités de Vichy ou les forces d'Occupation, la recherche de la destination des biens ayant fait l'objet de ces spoliations, et l'inventaire de ceux de ces biens qui n'ont pas été restitués ;

Considérant que les informations nominatives faisant l'objet de ce traitement font apparaître que les personnes concernées ont été considérées comme juives par les autorités de Vichy ou les forces d'Occupation ; qu'en application de l'article 31 de la loi du 6 janvier 1978, le traitement de telles informations est interdit sauf accord exprès des intéressés à moins qu'il n'ait

été fait exception à cette interdiction pour des motifs d'intérêt public, par décret en Conseil d'État pris sur proposition ou avis conforme de la Commission ;

Considérant que le consentement exprès des intéressés, dont la plupart sont décédés, ne peut être recueilli ; que l'objectif poursuivi, qui consiste à permettre l'évaluation des spoliations réalisées à l'encontre de personnes ayant fait l'objet de mesures discriminatoires du seul fait qu'elles ont été considérées comme juives, relève de l'intérêt public ;

Considérant toutefois que la finalité du traitement ne rend pas nécessaire la collecte et le traitement d'informations relevant de l'ensemble des catégories mentionnées à l'article 31 de la loi du 6 janvier 1978, mais seulement du fait que les personnes victimes de spoliation ont été considérées comme juives par les autorités de Vichy ou les forces d'Occupation ; qu'il y a lieu, dès lors, de modifier sur ce point la rédaction du projet ;

Émet un avis favorable sur le projet de décret sus-analysé dans la rédaction suivante :

« En application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 susvisée, la mission d'étude sur la spoliation des personnes considérées comme juives par les autorités de Vichy, ainsi que les personnes travaillant pour son compte et sous son contrôle, sont autorisées à collecter et à traiter des informations faisant apparaître directement ou indirectement l'origine des personnes résidant en France, considérées comme juives par les autorités de Vichy et ayant subi des spoliations de la part de ces autorités et des forces d'Occupation, au seules fins d'évaluer l'ampleur des spoliations, de rechercher la destination pendant l'Occupation et après la fin de la guerre des biens ayant fait l'objet de ces spoliations et d'inventorier ceux de ces biens qui n'ont pas fait l'objet de restitutions. »

Délibération n° 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

(Demande d'avis n° 553 059)

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 son article 31 ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

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

Vu l'arrêté du 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 le projet d'arrêté présenté par le Premier ministre ;

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

Considérant que la Commission est saisie par le Premier ministre d'une demande d'avis relative à un traitement dont la finalité est de permettre l'évaluation de l'ampleur des spoliations subies par les personnes considérées comme juives par les autorités de Vichy ou les forces d'Occupation, la recherche de la destination des biens ayant fait l'objet de ces spoliations pendant l'Occupation et la fin de la guerre, et l'inventaire de ceux de ces biens qui n'ont pas été restitués ;

Considérant que ce traitement doit être mis en œuvre pour les besoins de la mission d'étude sur la spoliation des juifs de France créée par arrêté du 25 mars 1997 ; que les ordinateurs utilisés pour la création des fichiers seront implantés aux Archives de France, à la Caisse des dépôts et consignations et à la préfecture de police, qui détiennent les archives à exploiter ;

Considérant que les catégories d'informations appelées à figurer dans ce traitement informatique sont relatives, s'agissant des personnes spoliées, à leur nom, prénom, adresse, profession, date et lieu de naissance, nationalité, fichage éventuel, nom et prénom des membres de la famille, nom et prénom des personnes qui se sont éventuellement déclarées comme ayants-droit à la libération, sort de la personne et des membres de la famille pendant et après la guerre ;

Considérant que les informations relatives aux biens dont les propriétaires ont été dépossédés, que ces biens aient été mis sous séquestre ou administrés par des tiers, sont les nom et qualité des dépositaires et administrateurs provisoires et les opérations effectuées sur les biens par les dépositaires et administrateurs provisoires ;

Considérant que les informations sur les restitutions opérées après la guerre sont relatives à l'identité des personnes ayant réclamé le bien, ainsi que des personnes appelées à le restituer ;

Considérant que ces informations proviennent des dossiers détenus par les divers fonds d'archives : Archives de France, Caisse des dépôts et consignations, préfecture de police, Centre de documentation juive contemporaine, ministère des Anciens combattants ;

Considérant que les informations nominatives faisant l'objet de ce traitement font apparaître que les personnes concernées ont été considérées comme juives par les autorités de Vichy ; que par délibération n° 97 092 en date de ce jour, la Commission a donné un avis favorable à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 autorisant la collecte et le traitement de telles données ;

Considérant que les destinataires des informations nominatives traitées seront les membres de la mission désignés par l'arrêté du 25 mars 1997 ainsi que les personnes qui travaillent directement pour son compte et sous son contrôle (les chercheurs et enseignants-chercheurs mandatés par le président de la mission), les personnels relevant des divers ministères et organismes (ministère de la Justice, ministère de la Défense ministère des Affaires étrangères, ministère de l'Intérieur, ministère de l'Economie, des Finances et de l'Industrie, ministère de la Culture et de la Communication, secrétariat d'état aux Anciens combattants, Banque de France, Caisse des

dépôts et consignations, Centre de documentation juive contemporaine) à la condition d'être mandatés par le président de la mission ;

Considérant que les personnes concernées pourront, conformément au chapitre V de la loi n° 78-17 du 6 janvier 1978, exercer leur droit d'accès auprès du président de la mission ;

Émet un avis favorable sur le projet d'arrêté présenté par le Premier ministre sous réserve que le projet de décret, portant application des dispositions du troisième alinéa de l'article 31 de la loi 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, adopté par délibération de la Commission n° 97 092 en date de ce jour, soit signé par le Premier ministre et publié au Journal officiel.

B. La recommandation sur les bases de données comportementales

Les bases de données utilisées pour le marketing direct se sont radicalement transformées sous l'effet d'une double évolution : d'une part, la volonté non plus d'atteindre un maximum de clients potentiels, mais de cibler les consommateurs ; d'autre part, les progrès considérables des méthodes d'exploitation des informations. Ainsi, en quelques années, les fichiers traditionnels du marketing direct, qui recensaient un nombre limité d'informations par personne, ont été remplacés par des mégabases de données dont la particularité est précisément d'abriter le plus grand nombre de renseignements sur les individus en vue de les répertorier ou de les classer selon certains « profils » (cf. 15e rapport, p. 182 et 16e rapport, p. 121).

En effet, ces mégabases de données personnelles sont susceptibles de rendre compte tout à la fois des habitudes de consommation (équipement de la maison, centres d'intérêt, alimentation, soins du corps, animaux, voiture...) et du comportement général (profession, environnement familial, propriétaire ou locataire, revenus...). De plus, au-delà du profil d'un individu qui peut être ainsi déterminé et cédé, de manière assez classique, à des tiers souhaitant cibler leurs opérations de prospection, c'est également le profil d'un groupe qui peut être établi grâce au procédé du géomarketing qui permet d'analyser statistiquement le profil de consommation par quartier. Il est également possible que l'exploitation des données nominatives puisse servir à d'autres fins, pour établir par exemple des statistiques par marque ou par produit.

La CNIL a, dès l'émergence des mégabases, été saisie de nombreuses plaintes à l'égard des sociétés qui constituaient ces gigantesques fichiers ; toutefois, il s'est avéré que les informations nominatives qui servaient à les alimenter étaient recueillies grâce à des questionnaires diffusés anonymement à des millions d'exemplaires. Généralement, des cadeaux, bons d'achat ou autres chèques de réduction à valoir sur de futurs achats sont proposés aux consommateurs afin de les inciter à répondre à quelque deux cents questions.

Dans la mesure où la collecte de ces données est facultative, la Commission s'est surtout attachée à veiller à ce que les consommateurs soient parfaitement informés, d'une part de ce que leurs réponses sont appelées à alimenter une base de données comportementales destinées à être commercialisées et, d'autre part, de leur droit de s'opposer à toute cession à des tiers d'informations les concernant. À cet égard, la CNIL a demandé que figure sur les questionnaires diffusés une case à cocher destinée à faciliter l'expression du droit d'opposition. D'ailleurs, la directive européenne, qui doit être prochainement transposée en droit français prévoit, dans son article 14, que toute personne puisse s'opposer, sur demande et gratuitement, au traitement des données la concernant à des fins commerciales ou soit informée de ses droits préalablement à la première communication à un tiers ou utilisation à des fins commerciales de ces données. En pratique, la Commission est extrêmement attachée à l'apposition d'une case à cocher sur ce type de questionnaire parce qu'elle permet aux personnes de manifester, sur le même support que celui de leurs réponses, leur opposition à la cession de leurs données à des sociétés extérieures et les dispense donc d'avoir à accomplir une formalité supplémentaire ou d'engager une dépense pour exercer leur droit.

Toutefois, dans la mesure où la CNIL avait à connaître d'un nombre croissant de déclarations concernant des mégabases de données personnelles et de nombreuses plaintes, elle a souhaité rappeler, par le biais d'une recommandation de portée générale, quelques principes élémentaires de protection des données personnelles et inciter les opérateurs à adopter des méthodes permettant de les respecter.

Ainsi, la recommandation du 18 février 1997 a mis l'accent sur la loyauté de la collecte, exigée par l'article 25 de la loi du 6 janvier 1978 et l'article 5 a de la Convention du Conseil de l'Europe, puis réaffirmé par la directive européenne du 24 octobre 1995. À cet égard, la CNIL a estimé que les consommateurs doivent avoir parfaitement conscience de ce que leurs réponses vont alimenter des fichiers de prospection commerciale. C'est dans cet esprit que la Commission s'attache particulièrement à l'obligation de porter sur les questionnaires des mentions d'informations claires et lisibles. De même, la CNIL a rappelé la nécessité que les personnes puissent exprimer leur opposition à une cession de leurs données à des tiers sans avoir à accomplir de démarches supplémentaires. Cette recommandation, publiée *au Journal officiel en* date du 9 septembre 1997, entend ainsi faire progresser la protection des données personnelles dans un secteur qui, par nature, est fortement consommateur d'informations nominatives.

D'ores et déjà, cette recommandation constitue sans aucun doute une première réponse aux gigabases du réseau Internet et à sa puissance de collecte et d'exploitation des données. En effet, l'éventail des informations personnelles qui peuvent être recueillies auprès d'un utilisateur du réseau des réseaux s'avère extrêmement large : nom, prénom, adresse postale, adresse électronique, adresse de livraison du bien ou service, information relatives au paiement (prix, mode de paiement, numéro de carte de paiement), informations relatives au

comportement d'un utilisateur lorsqu'il choisit de se connecter sur un site et qui permettent de révéler ses choix, ses préférences et ses affinités, le moment et la durée de la connexion. De plus, l'immense majorité des questionnaires en ligne incitent l'internaute à remplir des champs « commentaire libre » dans lesquels il peut communiquer sans restriction toutes informations qu'il jugerait utiles.

Au final, la constitution de réservoirs de données personnelles, via Internet peut, si l'on y prend garde, faire peu de mystère du droit à la vie privée des internautes ! (*cf. infra* 2e partie, chapitre 1).

Aussi, la CNIL a sans plus attendre adapté au réseau des réseaux, des réponses fournies par des dispositions de la loi du 6 janvier 1978 : il s'agit notamment de l'obligation de sécurité à la charge des responsables de traitements et des règles applicables à la collecte des données.

Toutefois, la dimension mondiale de l'Internet nécessite de s'entendre sur le niveau minimum requis en matière de protection des données que les pays européens souhaitent exiger des États qui ne sont pas encore dotés d'une législation spécifique dans ce domaine ou des opérateurs installés sur le territoire de ces États. En effet l'article 25 de la directive du 24 octobre 1995 pose le principe que les transferts internationaux de données ne peuvent avoir lieu que si le pays destinataire assure une protection adéquate au regard des règles européennes : cela paraît bien constituer désormais une priorité dans l'édification d'une société mondiale de l'information respectueuse de la personne humaine (*cf. infra* 2e partie chapitre 2).

Délibération n° 97-012 du 18 février 1997 portant recommandation relative aux bases de données comportementales sur les habitudes de consommation des ménages constituées à des fins de marketing direct

La Commission nationale de l'informatique et des libertés,

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

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

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

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

Considérant que la Commission a été saisie de la constitution de bases de données nominatives relatives aux habitudes de consommation des ménages, créées par des sociétés de marketing direct à des fins de prospection commerciale ;

Considérant que ces bases de données reposent sur la diffusion massive de questionnaires comportant des dizaines de questions (parfois plus de cent-cinquante par questionnaire), distribués anonymement à des millions d'exemplaires, par insertion dans des magazines ou par distribution dans les boîtes aux lettres ou sur des points de vente (commerces, supermarchés, etc.) ;

Considérant que ces questionnaires sont le plus souvent présentés par les organismes qui les diffusent comme des enquêtes sur la consommation, des études sur la qualité des produits, voire des sondages ;

Considérant que pour inciter les consommateurs à répondre à ces questionnaires, il leur est proposé, en contrepartie de leur « participation », des cadeaux, des bons d'achats ou des chèques de réduction à valoir sur des achats futurs ;

Considérant que si la diffusion de ces questionnaires est anonyme et les réponses facultatives, leur objet même vise à recueillir le plus grand nombre possible de coordonnées de consommateurs (nom et adresse) et le plus de renseignements possibles sur les personnes qui y répondent ;

Considérant en effet que les bases de données constituées à partir des réponses reçues des consommateurs qui ont rempli les questionnaires ont notamment pour finalité de constituer des profils de consommateurs et. de commercialiser les informations nominatives recueillies en les cédant ou en les mettant à la disposition d'annonceurs souhaitant les démarcher ;

Considérant que l'article 5 de la Convention du 28 janvier 1981 du Conseil de l'Europe et l'article 25 de la loi du 6 janvier 1978 font obligation aux responsables de fichiers de collecter les données nominatives de manière loyale ;

Considérant que l'article 27 de la loi du 6 janvier 1978 fait obligation aux responsables de traitements de mentionner sur tout questionnaire de collecte de données, non seulement le caractère obligatoire et facultatif des réponses et le lieu où s'exerce le droit d'accès mais aussi les catégories de destinataires des données ;

Considérant que l'article 2-2 du code de déontologie des professionnels du marketing direct publié le 8 décembre 1993 par l'Union française de marketing direct préconise que soit clairement indiqué aux personnes qu'elles peuvent s'opposer à ce que leurs nom et adresse soient cédés ou mis à la disposition d'autres sociétés et ce, préalablement à la première cession ;

Considérant que s'agissant de questionnaires comportant plusieurs dizaines de questions relatives au comportement privé des intéressés et diffusés à des millions d'exemplaires, la Commission doit veiller tout particulièrement à ce que les données soient obtenues et traitées loyalement, que l'adhésion des personnes à l'opération soit sincère et éclairée et que les droits des personnes à l'égard du traitement des données puissent s'exercer aisément ;

Recommande :

Que la présentation des questionnaires diffusés soit dépourvue de toute ambiguïté sur la finalité de la collecte des informations et, en particulier, que l'emploi de tout terme ou appellation de nature à créer une confusion dans l'esprit du public, telle l'appellation « Institut » ou le terme « sondage », pouvant laisser croire inexactement à une finalité statistique voire officielle ou ayant pour objet de dissimuler la réalité commerciale de l'opération, soit évité ;

Que la présentation des questionnaires ne comporte aucune ambiguïté sur la finalité des bases de données qui sont constituées à partir des réponses fournies par les consommateurs, de sorte que ces derniers aient clairement conscience que leurs réponses sont appelées à alimenter des fichiers de prospection commerciale ;

Que les questionnaires soient présentés de telle manière que les personnes concernées, lorsqu'elles sont incitées à y répondre en contrepartie d'offres diverses (cadeaux, bons d'achats ou coupons de réduction) soient clairement informées des conditions dans lesquelles elles pourront bénéficier de ces offres ; que tel doit être tout particulièrement le cas lorsque ces offres sont réservées aux seules personnes ne s'étant pas opposées à la cession de leurs données à des sociétés extérieures ;

Que les mentions d'information des personnes prévues par l'article 27 de la loi du 6 janvier 1978 et tout particulièrement l'indication que des sociétés extérieures pourront être destinataires des informations les concernant, sauf opposition de leur part, soient portées de manière claire et lisible sur les questionnaires ;

Que les consommateurs puissent exprimer aisément, sans avoir à accomplir de démarche supplémentaire, leur opposition à ce que des sociétés commerciales, autres que l'organisme qui procède au recueil de données, soient destinataires des informations nominatives les concernant ; Que les personnes intéressées soient informées, en tête du questionnaire, qu'elles peuvent répondre aux questions tout en s'opposant, notamment par l'apposition d'une case à cocher, à la cession de leurs données à des tiers et des conséquences à leur égard d'un refus de cession.

III. LES DECISIONS JURIDICTIONNELLES RELATIVES À L'APPLICATION DE LA LOI

Les décisions de justice commentées ci-après sont reproduites en annexe 7 de ce rapport.

A. Les formalités préalables

ARRÊT DU CONSEIL D'ÉTAT, 6 JANVIER 1997
(Section du contentieux)

Un arrêt du Conseil d'État du 6 janvier 1997 a tranché le problème des pouvoirs de la CNIL en matière de déclaration ordinaire prévue par l'article 16 de la loi du 6 janvier 1978.

En effet, à l'occasion d'un recours pour excès de pouvoir formé par la Caisse d'épargne Rhône-Alpes-Lyon contre une décision implicite de refus de la CNIL de délivrer le récépissé d'une déclaration de traitement, le Conseil d'État a précisé que dès lors que le dossier de déclaration est complet au regard de

l'article 19 de la loi du 6 janvier 1978 et que celui-ci comporte l'engagement que le traitement satisfait aux prescriptions de la loi, la CNIL est tenue de délivrer sans délai le récépissé de déclaration.

Cet arrêt met un terme à la pratique de la CNIL qui, soucieuse de veiller, dès le stade de leur mise en œuvre, à la régularité des traitements d'informations nominatives des entreprises du secteur privé, informait à l'occasion de l'instruction des dossiers de déclaration, les responsables de traitements de leurs obligations, comme l'article 6 de la loi du 6 janvier 1978 l'en charge au demeurant.

Il pouvait alors advenir, dans de rares cas où la méconnaissance de la loi lui paraissait caractérisée, que la Commission refuse de délivrer le récépissé ou suspende cette délivrance jusqu'à ce que le responsable du traitement, mieux informé des prescriptions de la loi, modifie les caractéristiques de son projet afin de le rendre conforme aux exigences de la protection des données. C'est cette pratique que le Conseil d'État a sanctionné.

B. Le droit d'opposition

ARRÊT DE LA COUR D'APPEL DE VERSAILLES, 2 JUILLET 1997

Cet arrêt non définitif, la société mise en cause ayant formé un pourvoi en cassation, s'ajoute à quelques décisions judiciaires déjà rendues sur le problème de l'utilisation par des tiers, à des fins commerciales, de l'annuaire électronique des abonnés au téléphone fixe diffusé par France Télécom sur le 3611.

Une société avait en effet procédé au téléchargement de l'annuaire diffusé par France Télécom pour constituer, pour son propre compte, une base de données commerciales, destinées à être cédées ou vendues à des tiers.

Initialement poursuivie pour mise en œuvre de traitements d'informations nominatives malgré l'opposition des personnes (en l'espèce, les abonnées inscrits en liste orange, l'article R. 10-1 du code des postes et télécommunications interdisant l'utilisation par quiconque à des fins commerciales des données les concernant), la société mise en cause a été relaxée par la juridiction du premier degré. France Télécom, partie civile, et le ministère public ayant interjeté appel de cette décision, la cour d'appel de Versailles a été amenée à rejuger cette affaire.

Infirmant la décision des premiers juges, la cour d'appel retient de l'article R. 10-1 du code des postes et télécommunications que « le refus des abonnés au téléphone de recevoir des sollicitations commerciales constitue, dès lors qu'il tend à la protection de la vie privée, un motif légitime d'opposition à l'utilisation de données nominatives les concernant [...] et que l'obligation s'impose à tous de respecter l'opposition manifestée en ce sens par ces personnes auprès de l'exploitant public ». Telle avait d'ailleurs été le fondement de la dénonciation par la CNIL de cette société au parquet (cf. 15^{e} rapport d'activité, p. 91 à 97).

L'exposé des motifs de cette décision est cependant nuancé, la cour d'appel de Versailles soulignant qu'il appartiendra « le cas échéant » à la juridiction compétente de sanctionner la pratique consistant pour France Télécom « seul détenteur des données publiques de l'annuaire et des informations relatives aux abonnés inscrits en liste orange à refuser à des entreprises concurrentes sur le marché du marketing direct l'accès à ces informations ». Ce considérant est à rapprocher du dispositif de la recommandation n° 97-60 du 8 juillet 1997 relative aux annuaires en matière de télécommunications qui préconise, notamment, que les personnes inscrites en liste orange soient identifiées sur tous les annuaires diffusés, quel qu'en soit le support.

On relèvera enfin que la juridiction d'appel, rejetant le fait justificatif allégué par la société mise en cause (l'état de nécessité), affirme que les agissements de cette société ne peuvent justifier qu'il soit porté atteinte « au principe supérieur de la liberté individuelle et de la protection de la vie privée ».

ARRÊT DU CONSEIL D'ÉTAT, 30 JUILLET 1997
(10e et 7e sous-sections réunies)

La société Consodata contestait devant le Conseil d'État le bien fondé de l'avertissement qui lui avait été adressé par la CNIL en application de l'article 21-4e de la loi du 6 janvier 1978, pour avoir supprimé des questionnaires sur les habitudes de consommation des ménages qu'elle diffusait à des millions d'exemplaires, la case à cocher destinée à permettre aux personnes d'exprimer immédiatement leur opposition à ce que les données les concernant soient cédées à des tiers.

Cet arrêt revêt une grande importance dans la mesure où il s'agit de la première délibération, portant avertissement de la CNIL qui soit déféré à la censure du Conseil d'État.

Il résulte de l'arrêt du 30 juillet 1997, en premier lieu, que l'avertissement délivré par la CNIL constitue une mesure faisant grief susceptible de recours devant la juridiction administrative.

En deuxième lieu et sur le fond, le Conseil d'État confirme le bien fondé de l'avertissement adressé par la CNIL dans des termes qui méritent de retenir l'attention.

D'une part, le Conseil d'État juge que la suppression de la case à cocher et sa substitution par une mention informant les personnes interrogées qu'elles pouvaient, en écrivant à la société Consodata, s'opposer à la communication à des tiers d'informations nominatives les concernant, constituaient une « caractéristique essentielle du traitement » et que, dès lors, la société Consodata était tenue de déclarer le nouveau traitement à la CNIL, dans les formes prévues par les articles 16 et 19 de la loi.

D'autre part et surtout, le Conseil d'État a estimé que « la suppression de la case à cocher [...] avait pour objet et pour effet de réduire le nombre de

personnes interrogées par questionnaire manifestant leur opposition à la cession à des tiers des données nominatives les concernant », ce qui était très exactement ce contre quoi la CNIL avait souhaité réagir en délivrant l'avertissement.

Depuis lors, la société en cause a régularisé sa situation en apposant à nouveau une case à cocher sur les questionnaires diffusés.

C. Le droit d'accès

ARRÊT DU CONSEIL D'ÉTAT, 29 DÉCEMBRE 1997
(10e et 7e sous-sections réunies)

Le requérant, qui avait présenté une demande de droit d'accès à des fichiers relevant de la sûreté de l'État, de la défense et de la sécurité publique, avait attaqué la décision de la CNIL lui notifiant, dans les termes prévus par l'article 39 de la loi du 6 janvier 1978, « qu'il avait été procédé aux vérifications » sans lui donner connaissance, ce que n'autorise pas la loi, des constatations faites par la CNIL, non plus que des éventuelles rectifications qui auraient, à cette occasion, pu être apportées aux fichiers en cause.

Le Conseil d'État avait déjà jugé que la procédure instituée par l'article 39 de la loi du 6 janvier 1 978 en matière de droit d'accès aux fichiers relevant de la sûreté de l'État, de la défense et de la sécurité publique était conforme à la Convention européenne, de sauvegarde des Droits de l'homme. Dans le présent arrêt, le Conseil d'État juge que cette procédure n'est « pas incompatible » avec les dispositions de la Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée le 28 janvier 1981 et ratifiée par la France, que l'on nomme communément Convention 108.

Cette décision est à rapprocher des commentaires sur la transposition de la directive (cf. *supra,* I).

D. La communication d'informations à des tiers

ARRÊT DU CONSEIL D'ÉTAT, 28 MARS 1997
(10e et 7e sous-sections réunies)

L'article L. 1611.4 du code général des collectivités territoriales (qui a remplacé l'article L. 221-8 du code des communes) reconnaît à l'autorité communale le pouvoir d'exiger d'une association recevant une subvention de la commune, la copie certifiée du budget et des comptes de l'exercice écoulé ainsi que la communication de tous documents faisant apparaître les résultats de l'activité de l'association.

La CNIL, saisie de nombreuses demandes de conseil de maires souhaitant obtenir, sur le fondement de ces dispositions, communication de la liste des

membres d'une association sollicitant une subvention, recommandait jusqu'alors que le maire ou un de ses représentants puisse consulter, au siège de l'association, la liste de ces membres mais sans pouvoir en prendre copie. Dans son arrêt du 28 mars 1997, le Conseil d'État se montre plus rigoureux et juge que la communication à l'autorité communale de la liste des adhérents d'une association, même subordonnée à l'interdiction faite à la commune d'en garder copie, méconnaissait le principe de la liberté d'association, lequel a valeur constitutionnelle.

E. Les sondages

ARRÊT DU CONSEIL D'ÉTAT, 9 JUILLET 1997
(Section du contentieux)

Cet arrêt tranche un délicat problème sur lequel la Commission avait eu à se pencher dès 1983, à l'occasion de demandes d'interprétation de la loi du 6 janvier 1978 dont elle avait été saisie par diverses personnalités sur le compte desquelles des sondages, non publics, avaient été opérés.

Les résultats des sondages sur ces personnalités constituaient-ils, à leur égard, des informations nominatives au sens de la loi du 6 janvier 1 978 ? Le commanditaire du sondage devait-il ou non être considéré comme destinataire d'informations nominatives concernant ces personnalités ? Répondre par l'affirmative revenait à reconnaître aux personnes concernées (candidats, élus etc.) sur le compte desquelles un sondage était effectué, le plus souvent par un probable concurrent, le droit de connaître les résultats les concernant et le commanditaire.

En 1993 la chambre syndicale des sociétés d'études et de conseils (SYNTEC) a saisi la CNIL d'une demande de conseil en souhaitant voir révisée la position prise par la Commission en 1983 *(cf.* 14e rapport d'activité, pages 215 à 218). C'est la confirmation de cette position ancienne, mais rédigée en termes plus généraux, qui a été attaquée par le Syntec devant le Conseil d'État.

L'arrêt du Conseil d'État annule la délibération contestée au motif « qu'un sondage comportant des questions qui demandent aux personnes ce qu'elles pensent d'une personnalité ne contient pas d'informations qui s'appliquent à celles-ci au sens de l'article 4 de la loi du 6 janvier 1978 » et en conclut que « la personnalité sur le compte de laquelle un sondage est effectué ne peut avoir accès à ce sondage sur le fondement de l'article 34 de la loi du 6 janvier 1978, ni exiger de savoir qui a commandé ledit sondage à l'institut qui l'a réalisé ».

Chapitre 3

LA PROTECTION DES DONNÉES EN EUROPE ET DANS LE MONDE

I. LES LEGISLATION NATIONALES

Tous les pays de l'Union européenne sont désormais dotés d'une législation générale de protection des données. Depuis 1994, la CNIL présente dans son rapport d'activité un récapitulatif de ces législations nationales, assorti des dernières modifications éventuelles. À cette occasion, sont mentionnées la situation de chaque État de l'Union au regard de la ratification de 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, les références de la ou des lois nationales de protection des données, ainsi que la dénomination et l'adresse de l'autorité nationale de protection des données. Il convient de noter que les lois de l'Italie et de la Grèce, adoptées respectivement en 1996 et 1997, c'est-à-dire postérieurement à la directive européenne du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données, sont déjà conformes à celle-ci. Les autres pays ont pour la plupart engagé la procédure de transposition des normes communautaires de protection des données dans leur droit national. Il semble que le Royaume-Uni soit à cet égard le plus avancé dans la mesure où le projet de loi britannique a été déposé devant la Chambre des Lords (texte disponible sur le site http://www.open.gov.uk) ; en revanche, l'Allemagne a annoncé un retard dans le calendrier de la transposition du fait des élections législatives de juin 1998. Par ailleurs, cette année, à l'heure de l'internationalisation des flux d'informations, la Commission a complété ce bilan par un panorama des autres pays du monde ayant adopté des règles de protection des données personnelles.

A. Dans l'Union européenne

ALLEMAGNE

Convention n° 108 ratifiée le 18 juin 1985, entrée en vigueur le 1er octobre 1985.

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.

Der Bundesbeauftragte fur den Datenschutz (autorité fédérale)
Postfach 200112
53131 Bonn

AUTRICHE

Convention n° 108 ratifiée le 30 mars 1988, entrée en vigueur le 1er juillet 1988.

Loi fédérale sur la protection des données du 18 octobre 1978, amendée en 1987 dans le sens d'un renforcement des règles en matière de flux transfrontières.

Direktor Buro der Datenschutzkommission und des Datenschutzrates
Bundeskanzleramt Ballhausplatz 1 1014 Vienne

BELGIQUE

Convention n° 108 ratifiée le 28 mai 1993, entrée en vigueur le 1er septembre 1993.

Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992.

Commission consultative de la protection de la vie privée Porte
de Hal 5-8 Bruxelles 1000

DANEMARK

Convention n° 108 ratifiée le 23 octobre 1989, entrée en vigueur le 1er février 1990.

Loi n° 293 du 8 juin 1978 sur les registres privés et loi n° 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées respectivement en 1988 afin de développer le droit d'accès des personnes et en 1991 en vue d'alléger les formalités préalables.

Registertilsynet Christians Brygge
28 4 sal 1559 Copenhague

ESPAGNE

Convention n° 108 ratifiée le 31 janvier 1984, entrée en vigueur le 1er octobre 1985.

Loi du 29 octobre 1992 portant réglementation du traitement automatisé de données personnelles.

Agencia de Protection de Datos Po de la
Castellana 41, 5. a planta, Madrid 28046

FINLANDE

Convention n° 108 ratifiée le 02 décembre 1991, entrée en vigueur le 1er avril 1992.

Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant le régime des fichiers de données nominatives mis en œuvre par la police.

Le médiateur à la protection des données
Albertinkatu 25 Boîte postale 315 00181
Helsinki

GRECE

Convention n° 108 ratifiée le 11 juin 1995, entrée en vigueur le 1er décembre 1995.

Loi n° 2472 sur la protection des personnes à l'égard du traitement des données à caractère personnel du 26 mars 1997.

Commission pour la protection des données 12,
rue Valaoritou 10671 Athènes

IRLANDE

Convention n° 108 ratifiée le 25 avril 1990, entrée en vigueur le 1er août 1990.

Loi sur la protection des données du 13 juillet 1988.

Data protection commissioner
Block 4, Irish Life Center Taibot
Street Dublin 1

ITALIE

Convention n° 108 ratifiée le 29 mars 1997, entrée en vigueur le 1er juillet 1997.

Loi n° 675 du 31 décembre 1996 sur la protection des données personnelles.

Garante per la protezione dei dati personali Via
della Chiesa Nuova, 8 00186 Rome

LUXEMBOURG

Convention n° 108 ratifiée le 10 février 1988, entrée en vigueur le 1er juin 1988.

Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, amendée en 1992 afin de renforcer la protection à l'égard des fichiers de police et des données médicales.

Commission consultative à la protection des données
Ministère de la Justice 16 boulevard Royal 2934 Luxembourg

PAYS-BAS

Convention n° 108 ratifiée le 24 août 1993, entrée en vigueur le 1er décembre 1993.

Loi du 28 décembre 1988 sur la protection des données, complétée en 1994 par des dispositions sur l'informatisation des registres communaux de population, et loi du 21 juin 1990 sur les fichiers des services de police.

Registratiekamer Prins
Clauslaan 20 Postbus 93374
2509 AJ's-Gravenhage

PORTUGAL

Convention n° 108 ratifiée le 02 septembre 1993, entrée en vigueur le 1er janvier 1994.

Loi n° 10/91 du 29 avril 1991 sur la protection des données à caractère personnel face à l'informatique, amendée par une loi du 29 août 1994 pour renforcer la protection à l'égard des données sensibles et en matière de flux transfrontières de données.

Comissào Nacional de Potecçào de Dados Informatizados 148,
rua de Sao Bento, 1200 Lisbonne.

ROYAUME-UNI

Convention n° 108 ratifiée le 26 août 1987, entrée en vigueur le 1er décembre 1987.

Loi sur la protection des données du 12 juillet 1984.

Data Protection Registrar
Wycliffe House
Water Lane Wilmslow Chesshire
SK9 5AF United Kingdom

SUEDE

Convention n° 108 ratifiée le 29 septembre 1982, entrée en vigueur le 1er octobre 1985.

Loi du 11 mai 1973 sur la protection des données.

Datainspektionen
Box 8114
104 20 Stockholm

B. Dans le monde

ARGENTINE

Loi sur la protection des données personnelles — 1996
(non promulguée à ce jour)

AUSTRALIE

Loi fédérale sur la vie privée -1978

Human rights and equal opportunity Commission
GPO Box 5218
Sydney NSW 1024

CANADA

Loi fédérale sur la protection des renseignements personnels — 1982

Federal privacy commission
Tower B, 3rd Floor, 112 Kent Street,
Otawa, Ontario K1A 1H3

ESTONIE

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)
(« The automated telephone consumer protection Act » -1991)

GUERNSEY

Loi sur la protection des données — 1986

The data protection officer
PO Box 43
La Charroterie
St Peter Port G71 1 FH

HONG-KONG

Loi sur la protection des données — 1990 Ordonnance sur la protection des données — 1995

Privacy commissioner for personal data Unit
2001, 20/F — Office Tower Convention
Plaza -1 Harbour Road Wan Chai — Hong-
Kong

HONGRIE

Convention n° 108 ratifiée le 08 octobre 1997, entrée en vigueur le 1er février 1998.

Loi sur la protection des données personnelles et la communication de données publiques — 1992

Parliamentary commissioner for data protection and freedom of information
Tük.ry 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

Convention n° 108 ratifiée le 25 mars 1991, entrée en vigueur le 1er juillet 1991

Loi n° 63-1981 relative à l'enregistrement de données personnelles — 1981 (amendée le 28 décembre 1989)

Icelandic Data Protection Commission
Arniarhvoll
150 Reykjav k

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

JAPON

Loi sur la protection des données informatisées à caractère personnel dans le secteur public — 1988

Governement information Systems planning division
Management and coordination agency
1-1 Kasumigaseki 3
Chiyoda-ku Tokyo
100 Japon

JERSEY

Loi sur la protection des données — 1987

Data protection registrar
States Greffe
Royal Square
St Helier JE1 1DD

MONACO

Loi n° 1 165 relative aux traitements d'informations nominatives — 1993

NORVEGE

Convention n° 108 ratifiée le 20 février 1984, entrée en vigueur le 1er octobre 1985

Loi sur les registres de données personnelles — 1978

Datatilsynet
Postboks 8177
Dep 0034, Oslo 1

NOUVELLE-ZELANDE

Loi sur la vie privée — 1993

Privacy commission
PO Box 466
Auckland

POLOGNE

Loi relative à la protection des données personnelles — 1997

REPUBLIQUE TCHEQUE

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 n° 24-FZ sur l'information, l'informatisation et la protection des informations — 1995

SLOVENIE

Convention n° 108 ratifiée le 23 novembre 1993, entrée en vigueur le 1er septembre 1994

Loi n° 210-01/89-3 sur la protection des données — 1990

SUISSE

Convention n° 108 ratifiée le 02 octobre 1997, entrée en vigueur le 1er février 1998

Loi fédérale sur la protection des données — 1992

Commissaire à la protection des données
Monbijoustrasse 5 3003 Berne

TAIWAN

Loi sur la protection des données — 1995

The ministry of justice
130, Sec 1, Chung Ching South Road
Taipei 100
Taiwan

II. LE DROIT COMMUNAUTAIRE

A. Le traité d'Amsterdam et la protection des données

Le traité d'Amsterdam prévoit que les institutions et organismes communautaires devront, à compter du 1er janvier 1999, respecter les normes communautaires en matière de protection des données, c'est-à-dire principalement la directive 95/46/CE relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données, adoptée le 24 octobre 1995 et publiée au *Journal officiel des Communautés européennes* du 23 novembre 1995 (cf. 16e rapport d'activité, p. 45 et annexe 10 ; *supra* chapitre 2).

Le traité prévoit également la création d'une autorité de contrôle indépendante, chargée de veiller au respect de la protection des données personnelles par les institutions et organismes communautaires.

B. La directive du 1er décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

Adoptée le 1er décembre 1997, la directive européenne concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications s'inscrit comme un texte complémentaire de la directive générale 95/46/CE relative à la protection des données personnelles. En effet, cette directive européenne s'attache à définir des mesures particulières de protection des personnes à l'égard des développements des télécommunications : identification de la ligne appelante, renvoi d'appel, annuaires, automates d'appel, utilisation des données de facturation... *(cf.* annexe 8).

Par ailleurs, il convient de rappeler l'adoption, le 17 février 1997, de la directive 97/7/CE concernant la protection des consommateurs en matière de contrats à distance (cf. annexe 8).

III. LA COOPERATION INTERGOUVERNEMENTALE

A. Schengen

La Convention d'application de l'accord de Schengen et du système d'information Schengen (SIS) est entrée en application, le 26 mars 1995. Ce système informatique permet de mettre en commun des informations détenues par les services de police de tous les « États Schengen » (10). À cet effet, le SIS comprend

une partie centrale, dénommée C-SIS qui est implantée à Strasbourg et placée sous la responsabilité de la France ainsi que des bases nationales, dénommées N-SIS, créées dans chaque État membre et constituant le reflet exact du C-SIS.

l'autorité de contrôle commune (ACC) instituée par l'article 115 de la Convention d'application, composée de deux représentants de chaque autorité nationale de contrôle, a été constituée en 1995. Les missions de cette autorité consistent à vérifier la bonne exécution des dispositions de la Convention à l'égard de la fonction de support technique (C-SIS) et à émettre des avis ou recommandations en cas de difficultés d'application ou d'interprétation par les États parties des dispositions de protection des données.

L'ACC a été présidée par M. Alex Tiirk, membre de la CNIL, de décembre 1995 à décembre 1997 ; ces fonctions sont actuellement exercées par M. Joao Labescat, membre de l'autorité de protection des données portugaise.

En 1997, l'ACC a élaboré un dépliant destiné à informer les citoyens de leurs droits. Ces dépliants sont destinés à être diffusés aux points de passages autorisés pour le franchissement des frontières extérieures de Schengen, notamment les aéroports.

L'autorité de contrôle commune vient de publier son deuxième rapport d'activité. Le texte et les annexes de ce rapport sont intégralement reproduits en appendice du présent rapport de la CNIL.

B. Europol

La Convention d'Europol qui a été signée le 26 juillet 1995 par les États membres vise à lutter contre la criminalité dans l'Union européenne et constitue à ce titre une étape importante dans la coopération policière européenne. Europol constitue le pendant européen de l'organisation internationale de police criminelle, Interpol, dont les fichiers sont encadrés par la Commission de contrôle des fichiers d'Interpol au sein de laquelle siège un membre de la CNIL, M. Michel Bernard.

Europol a pour mission de faciliter l'échange d'informations entre les États membres, en collectant, rassemblant et analysant des informations et des renseignements, puis en transmettant aux services compétents de chaque État membre les données qui les concernent. À cette fin, Europol est appelé à gérer un système informatisé d'informations, qui comprend, 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.

De nombreuses dispositions de cette Convention concernent la protection des données et son article 24 prévoit la création d'une autorité de contrôle commune composée de représentants des autorités nationales de protection des données. Constitué en son sein, un comité devrait être chargé d'examiner les recours présentés par les particuliers, en application des articles 19 et 20 de la Convention.

En 1997, les commissaires européens à la protection des données se sont réunis pour élaborer un projet de règlement intérieur que pourrait adopter la future autorité de contrôle commune.

IV. LE CONSEIL DE L'EUROPE

Afin de prendre en compte les progrès accomplis par la médecine et les technologies de l'information, le Conseil de l'Europe a adopté, le 13 février 1997, une recommandation n° R. (97) 5 relative à la protection des données médicales. Ce texte aborde notamment la question des données génétiques et des flux transfrontières de données de santé (cf. annexe 9).

V. LES CONFERENCES DES COMMISSAIRES À LA PROTECTION DES DONNÉES

A. La IV^{e} conférence européenne (Vienne)

La quatrième conférence européenne des commissaires à la protection des données s'est tenue à Vienne, les 24 et 25 avril 1997.

Dans un contexte de développement des réseaux et de mondialisation des flux d'informations, cette conférence a permis d'évoquer largement les réseaux d'informations, en particulier la question du chiffrement des données, les technologies visant à l'amélioration de la vie privée (« PETS »), et enfin, le commerce électronique.

La prochaine conférence européenne devait se tenir à Dublin, les 23 et 24 avril 1998.

B. La XIX^{e} conférence internationale (Bruxelles)

La XIX^{e} conférence internationale des commissaires à la protection des données a réuni à Bruxelles, du 17 au 19 septembre 1997, de nombreux membres et agents des autorités de protection des données, venus de 24 pays, ainsi qu'une centaine d'observateurs.

La conférence internationale a été notamment l'occasion de débattre des autoroutes de l'information et des flux transfrontières, de la directive européenne et de la notion de protection adéquate dans les pays tiers, de la protection de la vie privée et la liberté d'expression en particulier des journalistes, et bien sûr, de l'Internet.

Enfin, comme les années précédentes, les commissaires européens à la protection des données se sont rassemblés à l'issue de la conférence internationale, pour continuer à débattre de la transposition de la directive européenne et de l'état des réflexions des différents groupes de travail européens.

La prochaine conférence internationale doit se tenir à Saint-Jacques-de-Compostelle, du 16 au 18 septembre 1998.

LES ENJEUX

1997 aura été l'année de la protection des données personnelles sur Internet. Sans doute cette préoccupation ne s'est-elle pas imposée d'emblée lors des premiers balbutiements de l'entrée de l'Europe dans la société de l'information. Pour autant, les rapports annuels d'activité de la CNIL témoignent que, dès 1995, la Commission s'est prononcée sur des applications informatiques recourant à Internet. Il s'agissait alors de la diffusion des premiers annuaires — en l'espèce des annuaires de chercheurs — sur Internet. En 1996, le développement des applications sur le réseau ouvert et les procédures déclaratives prévues par la loi du 6 janvier 1978 ont permis à la Commission de mieux apprécier les enjeux de la matière, à l'occasion de l'ouverture de sites ministériels sur le « web », des premiers développements en France du commerce électronique ou des traitements de données personnelles mis en œuvre par les fournisseurs d'accès.

Parallèlement, la Commission s'est efforcée d'élargir sa réflexion au niveau européen et international en participant à de nombreux forums de discussion ou groupes de travail dont le GERI (Groupe européen d'études sur les réseaux internationaux), créé en 1995 à l'initiative de la CNIL et qui a réuni à plusieurs reprises des représentants de l'ensemble des autorités de protection des données des pays européens.

L'acquis de ces travaux, tout inspirés d'un souci de réalisme et de pragmatisme, a permis à la Commission d'enrichir sa réflexion et d'en faire part aux pouvoirs publics, soit directement, soit par l'intermédiaire des nombreux groupes de travail qui se réunissent sur le sujet.

À cet égard, la Commission se réjouit que le programme d'action gouvernemental intitulé « Préparer l'entrée de la France dans la société de

l'information », qui a été rendu public le 16 janvier 1998, fasse toute sa place au souci de la protection des données personnelles. Ce document précise en effet que « l'entrée dans la société de l'information se caractérise par un essor spectaculaire de la masse d'informations échangées sur les réseaux d'informations, et particulièrement des données personnelles dont la protection constitue un enjeu démocratique essentiel » (cf. p. 68).

Telle est en effet la conviction de la CNIL : il peut y avoir une société de l'information adaptée aux exigences de l'Etat de droit, qu'il convient de forger ensemble, en arrêtant des choix et en rendant des arbitrages sur quelques aspects fondamentaux des usages de l'Internet. Si cette réflexion ou ces choix n'étaient pas menés à leur juste terme, la société de l'information pourrait sombrer dans le tohu-bohu, un monde où la loi du plus fort, ou du mieux offrant, s'imposerait, ou encore dans un monde de surveillance. C'est à cette réflexion que la CNIL participe sur la base des compétences qui lui sont reconnues par la loi du 6 janvier 1978.

Mais cette « société de l'information » est, par nature, mondiale. Aussi, la réflexion ne peut-elle se borner aux frontières nationales, ni même aux limites de l'Europe. De ce point de vue, et même si les enjeux financiers, commerciaux, économiques ou industriels sont également considérables, la CNIL, avec les autres autorités de protection des données des États-membres de l'Union européenne, estime que la directive européenne du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données peut constituer un puissant levier pour convaincre de la justesse de l'approche européenne en la matière, qui est d'abord celle du droit au respect de sa personnalité et de sa vie privée.

Or, par ses caractéristiques, Internet, plus encore que toute autre technologie serait susceptible de constituer une menace si des protections n'étaient pas mises en œuvre.

La première caractéristique, liée à la nature même de ce réseau de communication ouvert, tient à ce que toute information qui y circule « en clair » peut être « télédéchargée » sur un micro-ordinateur depuis quelque endroit du monde que ce soit. Ainsi, la participation à un forum de discussion entre internautes peut être épiée par tous et les messages, laissés dans le contexte normalement éphémère d'une discussion, recopiés numériquement, classés, archivés, exploités (cf. 17^{e} rapport, p. 66). De même, la diffusion de données à l'échelle du monde, même si ces données revêtent un caractère public, peut présenter certains dangers. Ainsi, à titre d'exemple, les décrets de naturalisation font l'objet en France d'une publication obligatoire au Journal officiel ; la diffusion de textes d'une telle nature sur Internet pourrait offrir la possibilité à certaines officines d'identifier ceux des ressortissants de tel pays qui auraient souhaité renoncer à leur nationalité d'origine. Cet exemple — purement théorique et qui ne vaut que pour l'illustration du propos — manifeste que l'accessibilité mondiale des informations et les facilités de recherches sur Internet sont de nature à transformer une mesure de publicité, conçue comme une annonce de

bienvenue dans la communauté nationale à un ressortissant antérieurement d'une autre nationalité, en une véritable menace pesant sur l'intéressé qui acquiert la nationalité française. Cette caractéristique a d'ailleurs conduit les services du Journal officiel de la République Française à exclure spontanément la diffusion sur Internet des décrets de naturalisation, lors de la mise en ligne du Journal officiel sur le réseau.

La deuxième caractéristique du réseau est de générer un grand nombre de données transactionnelles qui sont nécessaires à son fonctionnement. Les techniques utilisées sur Internet pour établir la communication entre ordinateurs distants (protocole TCP/IP) reposant sur l'attribution d'une adresse dite « adresse IP » à chaque machine, l'acheminement d'un message ou la simple consultation d'un site par un internaute laisse une trace. Ainsi, les fournisseurs d'accès disposent de traitements, dénommés « fichiers log », qui permettent de tout connaître de l'internaute ou de reconstituer son activité : les sites qu'il a consultés, les pages du site sur lesquelles il s'est attardé, celles qu'il a négligées, le document qu'il aura téléchargé sur son micro, la date et l'heure de ses précédentes connexions.

Ces « fichiers log » constituent dès lors des gisements de données tout à fait considérables et détaillés, peuvent être exploités à des fins statistiques ; mais ils peuvent également être utilisés, à l'insu de la personne concernée, pour constituer des profils individuels de consommation ou repérer la navigation d'une personne sur Internet. Quelle doit être la juste durée de conservation de ces informations et à quelles fins peuvent-elles être utilisées (commerciales, de police et de repérage de la délinquance). Voilà également des questions qui touchent aux Droits de l'homme et qui sont au demeurant familières aux autorités de protection des données.

Sur ce point, les législations de l'ensemble des pays européens posent quelques principes élémentaires qui ont pu, dans le passé, s'adapter sans ajustement notable à l'ensemble des sauts technologiques, qu'il s'agisse des cartes à microprocesseur, de l'informatique en réseau, du minitel, ou de la micro-informatique. Face aux caractéristiques de ces techniques informatiques et aux dangers qu'elles recèlent pour la vie privée et la liberté individuelle, les États de l'Union européenne et quelques autres dans le monde se sont dotés d'instruments juridiques protecteurs à l'égard du traitement automatisé d'informations nominatives. Ces instruments juridiques doivent tout naturellement s'appliquer aussi à Internet, à ses dimensions mondiales, à ses capacités technologiques multipliées.

En France, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés offre de solides garanties juridiques. 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 constitue, au plan européen, le socle commun des garanties qui doivent être reconnues aux personnes.

Ainsi, la directive européenne précise que le responsable du traitement informatique doit informer la personne auprès de laquelle des données sont collectées des finalités du traitement auquel les données sont destinées (article 10), de son droit de s'opposer à ce que les données la concernant puissent être traitées à des fins de prospection commerciale, de son droit de s'opposer à ce que les données soient cédées à un tiers (article 12).

Le texte européen pose un autre principe fondamental : les données recueillies sur une personne dans un but déterminé doivent être utilisées exclusivement pour cette finalité et ne peuvent pas être ultérieurement traitées de manière incompatible avec la finalité initiale (article 6.1).

Enfin, la directive impose au responsable du traitement de prendre toute mesure pour assurer la sécurité des données nominatives, c'est-à-dire empêcher qu'elles ne soient altérées, détournées de leur finalité ou communiquées à des tiers qui n'auraient pas à en connaître.

Ces principes sont essentiels. Le 10e considérant de la directive européenne le rappelle opportunément : « l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire ». À l'occasion de leur dernière conférence qui s'est réunie à Dublin les 23 et 24 avril 1998, les commissaires européens à la protection des données ont adopté une résolution rappelant « que les règles de la protection des données personnelles, telles qu'elles résultent de la réglementation européenne, s'appliquent intégralement, selon des modalités appropriées, à toutes les informations fournies au réseau Internet ou transmises à ce réseau par quelque moyen, logiciel ou technique que ce soit ».

Mais au-delà des recommandations que la Commission a pu faire et qui sont consignées dans les chapitres qui suivent, la question se pose de savoir si le moment n'est pas venu d'élargir ensemble la réflexion ? En effet, les premières approches d'Internet par les pouvoirs publics ont été dictées par la préoccupation légitime de lutter contre tout usage illégal de ce nouveau mode de communication — diffusion de documents à caractère pédophile, de messages révisionnistes ou terroristes ; blanchiment d'argent, etc. La difficulté de repérer les activités illicites et d'en identifier leurs responsables a naturellement conduit à ce que toutes les personnes accédant à Internet et consultant ses différents services puissent être identifiées.

La préoccupation est incontestablement légitime. Pour autant, les activités sur Internet ne peuvent échapper à l'application des principes juridiques fondamentaux qui régissent les activités sociales dans une société démocratique. Internet ne saurait constituer un monde échappant aux règles normales d'un Etat de droit. S'il est évidemment légitime que l'autorité publique ait le souci qu'Internet ne devienne pas un refuge du crime, les moyens mis en œuvre pour atteindre cet objectif doivent être proportionnés et respecter l'article 6 de la

Convention européenne des Droits de l'homme. Des délinquants peuvent communiquer par courrier et la police n'ouvre pas toutes les lettres. Des criminels peuvent se téléphoner et l'on ne place pas toute une société sur écoute. Les restrictions qui peuvent être apportées à la vie privée ou aux libertés individuelles au motif de la lutte contre la délinquance doivent être strictement nécessaires à l'objectif que l'on s'assigne.

L'exploitation des informations circulant sur Internet, ainsi que la mémorisation des données transactionnelles et de connexion, pourraient transformer le cyberconsommafeur en objet de surveillance, le citoyen en individu épié. Peut-on admettre que le monde de l'Internet nous renvoie à celui des Incas où portes et fenêtres devaient être en permanence ouvertes pour que les inspecteurs de l'Inca puissent voir à tout instant ce qui se passait à l'intérieur des foyers ?

Au-delà des garanties juridiques mais aussi techniques qui paraissent de nature à éloigner le risque que présenterait ce monde virtuel, s'il devait s'affranchir de toute préoccupation de sauvegarde de notre vie privée, ces raisons ont convaincu la Commission nationale de l'informatique et des libertés, comme la plupart des autorités de protection des données des pays européens, que le moment était venu, non pas de jeter un voile d'anonymat sur la délinquance ou le crime, mais d'inciter à la reconnaissance d'un « *habeas corpus* de l'homme virtuel » qui reste encore à définir.

Permettre à la puissance publique d'exercer pleinement son rôle au plan de la sécurité dans tous les domaines est sans doute essentiel, mais comme dans toute société démocratique, la liberté doit être la règle et la coercition l'exception.

Par ailleurs, le caractère national et désormais européen des règles de protection des données personnelles ne suffit pas à rendre effectives les mesures destinées à assurer la loyauté de la collecte, à éviter les détournements de finalité ou à déterminer la juste durée de conservation des données sur un réseau mondial. À cet égard, la nécessité d'établir au plan international un corpus minimum de principes de protection des données et une coordination des États pour la poursuite et la répression de la violation de ces principes ne fait plus de doute.

L'adoption de la directive européenne du 24 octobre 1995 a, là encore, suscité une prise de conscience nouvelle de la part des États qui n'étaient pas encore dotés de législation générale en matière de protection des données. En effet, cette directive pose le principe que les transferts internationaux de données ne peuvent avoir lieu que si le pays destinataire assure une protection « adéquate » au regard des lois européennes. La crainte que les échanges commerciaux, notamment, puissent être suspendus ou interrompus sur la base de cette prescription a conduit les pays situés hors de la Communauté à se préoccuper de la protection des données personnelles.

Voilà pourquoi 1997 marque une date décisive dans la protection des données sur Internet.

De nombreuses associations d'internautes ou de consommateurs, surtout dans les pays qui ne sont pas dotés d'une législation en matière de protection

des données, préconisent la reconnaissance de principes inspirés par nos législations européennes. Au Japon, sous l'influence du Miti, ont été publiés des *guides-lines* transposant mot pour mot la directive européenne, à l'exception de celles de ses dispositions relatives aux sanctions et à l'institution d'une autorité de contrôle indépendante. Aux États-Unis, l'administration Clinton fait pression sur les industriels et les professionnels pour qu'ils prennent des mesures de protection des données susceptibles d'être considérées comme « adéquates » au sens des exigences européennes. Les pays de l'Europe centrale et orientale adhèrent de plus en plus nombreux à la Convention 108 du Conseil de l'Europe sur la protection des données. Les pays d'Amérique du Sud nouent des contacts avec les autorités européennes de protection des données. Dans la zone Asie-Pacifique, Hong-Kong, doté d'une loi de protection des données applicable au secteur public et au secteur privé, constitue une tête de pont, l'Australie et la Nouvelle-Zélande faisant par ailleurs figure de pionnier, dans cette partie du monde, en matière de protection des données.

Mais malgré ces avancées, la situation mondiale demeure marquée par une différence d'approche entre la philosophie européenne et celle, notamment des États-Unis, qui préconisent, plutôt que la définition de garanties légales, des mécanismes d'auto-régulation organisés par les professionnels eux-mêmes. De nombreuses discussions internationales ont lieu sur ce sujet dont il convient de rappeler les enjeux.

Ces réflexions liminaires sont poursuivies dans les deux chapitres qui suivent et qui n'ont été distingués que pour mieux marquer les deux écueils qu'il convient d'éviter.

Le premier écueil serait celui de la résignation : renoncer à toute règle au motif que les modalités de leur application au plan mondial seraient délicates à définir. Aussi, le chapitre premier est-il consacré aux recommandations de la CNIL dans divers domaines de la protection des données sur Internet.

Le deuxième écueil serait celui du manque d'audace : renoncer à faire prévaloir le socle de garanties définies au plan européen, au motif que des industries étrangères ou le marché rencontreraient des difficultés pour s'y adapter.

Il est enfin un dernier danger auquel la CNIL a toujours été sensible : celui du dogmatisme et de l'a *priori.* S'agissant de développements encore récents des usages d'Internet, le temps est évidemment celui de la réflexion ouverte avec les opérateurs et les citoyens. Mais la réflexion est toujours plus riche lorsqu'elle repose sur quelques solides convictions qu'énonce parfaitement l'article 1er de la loi du 6 janvier 1978 qui, malgré les considérables avancées technologiques, est plus que jamais d'actualité :

« 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 ».

Chapitre 1

LA PROTECTION DES DONNÉES À L'HEURE D'INTERNET

Ni la dimension mondiale des réseaux, ni leur ouverture totale, ni l'immédiateté de la communication qu'ils offrent n'empêchent que soient respectés sur Internet comme sur d'autres grands réseaux ouverts ou fermés (Intranet), les quelques principes fondamentaux de la protection des données personnelles qui sont appliqués dans la plupart des États européens et consignés dans la directive de 1995, à savoir : information des personnes, respect de la finalité du traitement, durée de conservation etc.

Aussi bien, les progrès fantastiques — et heureux — des technologies doivent-ils permettre d'appliquer concrètement ces principes, à la mesure même des capacités qu'elles ouvrent pour le traitement des données.

I. CITOYENS INTERNAUTES

L'utilisation du réseau Internet pour se rapprocher des administrés ou électeurs est devenue une priorité des pouvoirs publics, qui ont notamment manifesté la volonté de faciliter par Internet l'accès des citoyens à l'administration par Internet. Cela a conduit à l'ouverture de nombreux sites d'information, qui tantôt diffusent des données nominatives, par exemple des organigrammes, tantôt procèdent à la collecte de données personnelles, lorsqu'il s'agit par exemple d'effectuer des formalités administratives en ligne.

A. Les sites ministériels

La circulaire du Premier ministre, en date du 15 mai 1996, relative à la communication, l'information et la documentation des services de l'État, a demandé aux ministères de se doter de sites Internet avant le 31 décembre 1997.

Le site du Premier ministre et du Gouvernement a donné l'occasion à la CNIL de jeter les premiers fondements de sa doctrine en matière de protection des données sur Internet. Il convient de rappeler que la Commission a fait à cette occasion obligation aux fournisseurs de services sur Internet d'informer les personnes concernées des risques inhérents au réseau, préalablement ou au moment de leur utilisation et demandé que soient reconnu aux personnes le droit de s'opposer, à la diffusion d'informations les concernant, ceci sans avoir à en donner le motif (cf. 17^{e} rapport, p. 79).

Les positions prises par la Commission, en étroite concertation avec les services du Premier ministre, trouvent leur fondement dans les caractéristiques du réseau Internet que sont la possibilité de captation des informations diffusées et la difficulté, voire l'impossibilité, de contrôler l'utilisation qui pourrait être faite par des tiers des données diffusées sur Internet.

La Commission a ainsi considéré que le droit d'opposition visé à l'article 26 de la loi du 6 janvier 1978 devait trouver à s'appliquer, c'est-à-dire qu'il était a *priori* légitime de s'opposer à la diffusion de ses données sur ce réseau. La Commission a vu dans ce droit le seul moyen dont pouvaient, en pratique, disposer les personnes pour se prémunir contre les possibilités et les pratiques de téléchargement des bases de données et le détournement de leur finalité, dont les conséquences mettent en péril les droits qui leur sont reconnus par les règles nationales et internationales de protection des données.

Cette analyse se fonde notamment sur le constat que les pratiques de téléchargement ou les procédés de collecte systématique d'informations par les moteurs de recherche par exemple [1], rendent quasiment impossible le repérage de la collecte des informations diffusées et, dès lors, très difficile la sanction des détournements de finalité qui en découlent, à supposer même qu'une coordination policière et judiciaire internationale permette de l'envisager.

Elle se justifie, en outre, par l'absence généralement observée de niveau adéquat de protection offert par les pays tiers à partir desquels des données personnelles diffusées sur Internet peuvent faire, après avoir été collectées sur le réseau, l'objet de traitements échappant à toute règle propre à garantir les droits des personnes.

Ces règles ont été par la suite synthétisées lors de l'adoption d'un modèle type des traitements de données personnelles qui peuvent être créés sur un site

([1]) En indexant l'ensemble des données diffusées sur Internet, les moteurs de recherche rendent tout internaute, quelque soit sont lieu de situation sur la planète, des inataire de ces informa ions, ce qui, tout à la fois, constitue la caractéristique et l'intérêt essentiels d'un réseau International ouvert et rend indispensable la mise en œuvre d'un disposi if international de protection des données personnelles, du droit d'auteur, etc.

ministériel, modèle type destiné à simplifier les formalités administratives à accomplir auprès de la CNIL.

Ce modèle type précise que les serveurs d'informations peuvent contenir, notamment au titre de la communication ministérielle, la biographie du ministre et la composition de son cabinet (identité, photographie, fonction, attribution, titres, formation, distinctions, vie professionnelle et vie politique et, éventuellement, corps d'origine dans la fonction publique), son agenda (nom, fonction et titre de personnes n'appartenant pas à l'administration), les nominations en Conseil des ministres ; et pour les fonctionnaires, leurs identité, fonction, attribution, date de nomination et facultativement leur photographie.

Conformément à la doctrine de la CNIL, toutes les personnes concernées par ces services doivent être informées préalablement au chargement des informations sur le site, des risques inhérents à la diffusion d'informations sur Internet ainsi que, par voie de note de service, de leurs droits : d'une part, le droit de s'opposer à la diffusion d'informations les concernant, sans avoir à en donner le motif, ce droit pouvant s'exercer soit avant la diffusion, soit à tout moment ultérieur ; d'autre part, le droit d'accès et de rectification des données les concernant.

Par ailleurs, ce modèle type autorise la mise en place de forums de discussion sur des thèmes d'intérêt général. Dans le souci que les contributions déposées dans le cadre de ces forums puissent demeurer anonymes sans qu'il en résulte d'abus, la CNIL a admis qu'un modérateur puisse intervenir préalablement à la diffusion d'une contribution sur Internet, afin de contrôler si elle n'est pas de nature à engager la responsabilité civile et pénale du ministère ou si elle ne contient pas des informations sur des tiers qui pourraient porter atteinte à leur considération ou à l'intimité de leur vie privée (article 226-22 du code pénal). Les personnes doivent être informées de l'existence de ce modérateur et pouvoir en tout état de cause, si elles le souhaitent, participer au forum de discussion en s'identifiant.

La messagerie qui offre la possibilité d'adresser un courrier électronique au ministre ou à ses services, le cas échéant pour leur demander une documentation administrative, signale que le respect du secret des correspondances n'est pas garanti. Là encore, les personnes peuvent, dans la seule mesure où elles le souhaitent, accompagner tout message de leurs nom, adresse postale, adresse électronique, fonction et catégorie socio-professionnelle. Des mesures particulières ont été prévues pour protéger les mineurs à l'égard de tout détournement d'informations, en les invitant à ne divulguer que leur prénom ou à utiliser un pseudonyme. Des recommandations similaires ont été préconisées pour le service des jeux et concours.

Enfin, sur le plan technique, la CNIL a estimé que toutes les informations liées à la navigation sur un site ministériel (adresse IP, date et heure de la requête...), et qui sont utiles au fonctionnement et à la sécurité du site, ne devaient pas être conservées au-delà de quinze jours sur le site, qu'il soit hébergé ou non. De même, en cas d'hébergement du site, il est interdit au sous-traitant

d'utiliser ou de céder ces données. Ces données ne peuvent donc être exploitées qu'à des fins statistiques relatives à la fréquence de consultation des pages du site, à la nature des requêtes et à l'origine géographique des connexions qui est dévoilée par l'adresse IP de la machine.

Un avis favorable a été donné à ce modèle type de sites ministériels qui, au-delà de la simplification des formalités qu'il permet, constitue le socle de la doctrine de la CNIL dans ce domaine.

Délibération n° 97-009 du 4 février 1997 relative à la demande d'avis du Service d'information du Gouvernement concernant le traitement d'informations nominatives opéré dans le cadre du site Internet du Premier ministre et du Gouvernement
(Demande d'avis n° 483 293)

La Commission nationale de l'informatique et des libertés,

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 15, 26 et 29 ;

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

Vu le projet d'arrêté du Premier ministre ;

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

Considérant que la Commission a été saisie par le Service d'information du Gouvernement d'une demande d'avis relative à la création d'un traitement automatisé d'informations nominatives dans le cadre de la mise en œuvre du site Internet du Premier ministre et du Gouvernement ;

Considérant que le traitement a pour finalités la diffusion d'information au titre de la communication gouvernementale ainsi qu'au titre de l'information administrative, l'ouverture d'un espace de discussion pour les utilisateurs du site, la réception de courriers adressés au Premier ministre ou à ses services et l'organisation de concours ;

Considérant que la diffusion d'informations porte, au titre de la communication gouvernementale, sur la composition du Gouvernement et les cabinets, les agendas ministériels, les nominations en Conseil des ministres et, au titre de l'information administrative, sur les responsables et l'organigramme des services du Premier ministre ; qu'à cet égard, les informations diffusées relatives aux personnes physiques sont : pour les ministres et les membres de leurs cabinets, l'identité, la fonction, l'attribution, les titres, le corps de la fonction publique d'appartenance éventuellement, des informations biographiques sur leur formation, leur vie professionnelle et politique, les distinctions ; pour les fonctionnaires, l'identité, la fonction, le titre, la date de nomination ; pour les personnes figurant sur les agendas ministériels le nom, la fonction, le titre et l'organisme ; que ces informations sont d'accès libre ;

Considérant que ces personnes sont informées, avant mise sur le serveur des informations les concernant, des risques inhérents à la diffusion d'informations au moyen du média Internet ainsi que de leur droit de s'opposer à tout moment à la diffusion des informations qui les concernent sans avoir à en indiquer le motif ;

Considérant que l'ouverture d'un espace de discussion, pour les utilisateurs du site sur des thèmes d'intérêt général, peut conduire à la collecte et à la diffusion d'informations nominatives relatives à l'objet de la contribution, au nom et à l'adresse électronique de l'auteur ; que la consultation des contributions est libre ;

Considérant que les personnes adressant une contribution peuvent le faire, à leur choix, soit de manière anonyme, soit en indiquant, par exemple, leur nom ou leur adresse électronique ;

Considérant que cet espace de discussion fait l'objet d'une modération ; qu'à cet égard les contributions transmises, susceptibles d'engager la responsabilité civile et pénale du Service d'information du Gouvernement ne sont pas diffusées par le modérateur ; qu'en particulier une contribution contenant des informations relatives à un tiers, de nature à porter atteinte à sa considération ou à l'intimité de sa vie privée ne sera pas mise à la disposition du public ; que, de plus, afin d'empêcher la diffusion d'informations pouvant porter préjudice à un tiers dont l'identité aurait été usurpée ou l'intitulé de l'adresse électronique (e-mail) communiquée à son insu, il sera procédé en cas de doute à la vérification des informations auprès de la personne indiquée avant diffusion de la contribution concernée ;

Considérant que les utilisateurs du site accédant au forum sont informés de sa finalité, de ses règles de fonctionnement ainsi que des mentions prévues à l'article 27 de la loi du 6 janvier 1978 ;

Considérant que la durée de conservation des contributions émises dans le cadre du forum ne dépasse pas celle de l'inscription du thème du débat concerné ;

Considérant que les utilisateurs du site ont la possibilité de transmettre un courrier au Premier ministre ou à ses services au moyen d'une boîte aux lettres ; qu'ils sont avertis dès la page d'accueil du service des risques relatifs au secret des correspondances transmises sur Internet vers le site et qu'en conséquence il leur est conseillé de ne pas utiliser ce service pour des courriers de nature personnelle ;

Considérant que les personnes sont invitées à transmettre leur message, accompagné, si elles le souhaitent, de leur nom, de leur adresse de domicile, de leur adresse électronique, du nom de l'organisme au titre duquel elles adressent leur message, leur fonction, le motif et le sujet du message, leur catégorie socioprofessionnelle ; qu'il est explicitement indiqué que ces informations sont collectées de manière facultative ;

Considérant que les courriers ainsi recueillis sont transmis au service du courrier du Premier ministre qui le traite de la même manière que le courrier postal ;

Considérant que le site comporte également un espace destiné aux jeunes, dit « Espace juniors » destiné à les familiariser avec les services Internet publics ; que cet espace comporte la possibilité de transmettre un message au Premier ministre au moyen d'une boîte aux lettres spécifique, ainsi que de participer à des concours ;

Considérant que les utilisateurs de ces deux services sont susceptibles d'être des mineurs ; qu'en conséquence il leur est proposé de n'accompagner leur message, et de manière facultative, que de leur prénom ou d'un pseudonyme, de leur commune et pays de résidence, de leur âge et de leur classe ; qu'ils sont informés qu'aux fins de participer effectivement à un concours ils doivent en outre, avec l'accord de leurs parents, adresser leur réponse par courrier postal ;

Considérant qu'au-delà des mesures précitées destinées à garantir les droits des personnes, des mesures de sécurité offrant des garanties d'efficacité sont prises, notamment en vue d'empêcher des accès au site de nature à porter atteinte à l'intégrité des informations mises à la disposition du public ainsi qu'au détournement de finalité des informations recueillies sur le site ;

Considérant que la mise en œuvre des procédures de sécurité repose en particulier sur l'examen périodique des fichiers des connexions des utilisateurs au site conservés à cette fin ; que dans ces fichiers peuvent être conservés, au fur et à mesure des connexions des utilisateurs, notamment leur adresse Internet (adresse IP) ou celle de la machine à laquelle ils se connectent, le nom de domaine, la requête (page consultée, par exemple), la date et l'heure de la requête ;

Considérant que ces informations ne sont accessibles qu'au seul responsable de la sécurité ; que la durée de conservation des dites informations est de quinze jours et ainsi strictement limitée à celle nécessaire pour assurer la sécurité du site ;

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

Délibération n° 97-032 du 6 mai 1997 relative à la demande d'avis présentée par le Premier ministre concernant un modèle type de traitements d'informations nominatives opérés dans le cadre d'un site Internet ministériel

(Demande d'avis n° 520 219)

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 15, 26 et 29 ;

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

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ; Vu le projet d'arrêté du Premier ministre ;

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

Considérant que la Commission a été saisie par le Premier ministre d'une demande d'avis relative à la création de traitements automatisés d'informations nominatives mis en œuvre dans le cadre d'un site Internet ministériel ;

Considérant que ce modèle type, auquel tous les ministères qui souhaitent mettre en œuvre un tel site sur Internet pourront se référer, concerne

exclusivement les traitements ayant pour finalités la diffusion d'information au titre de la communication ministérielle, ainsi qu'au titre de l'information administrative, l'ouverture d'un espace de discussion pour les utilisateurs du site, la réception de courriers adressés au ministre ou à ses services et l'organisation de concours ;

Considérant que les informations diffusées concernent, au titre de la communication ministérielle, la biographie du ministre, la composition du cabinet du ministre, l'agenda du ministre, les nominations en Conseil des ministres intervenues dans le domaine de compétence du ministre et, au titre de l'information administrative, l'historique et l'organigramme du ministère ; qu'à cet égard, les informations diffusées relatives aux personnes physiques sont : pour le ministre et les membres de son cabinet, l'identité, la photographie, la fonction, l'attribution, les titres, le corps de la fonction publique d'appartenance éventuellement, des informations biographiques sur leur formation, leur vie professionnelle et politique, les distinctions ; pour les fonctionnaires, l'identité, la photographie, la fonction, les attributions, la date de nomination et le corps de la fonction publique d'appartenance ; pour les personnes figurant sur les agendas ministériels le nom, la fonction, le titre et l'organisme ; que ces informations sont d'accès libre ;

Considérant que ces personnes sont informées, avant mise sur le serveur des informations les concernant, des risques inhérents à la diffusion d'informations au moyen du média Internet ainsi que de leur droit de s'opposer à tout moment à la diffusion des informations qui les concernent sans avoir à en indiquer le motif ; que de surcroît, elles sont avisées que la production d'une photographie est facultative ;

Considérant que l'ouverture d'un espace de discussion pour les utilisateurs du site, sur des thèmes d'intérêt général, peut conduire à la collecte et à la diffusion d'informations nominatives relatives à l'objet de la contribution, au nom et à l'adresse électronique de l'auteur ; que la consultation des contributions est libre ;

Considérant que les personnes adressant une contribution peuvent le faire, à leur choix, soit de manière anonyme, soit en indiquant, par exemple, leur nom ou leur adresse électronique ;

Considérant que cet espace de discussion fait l'objet d'une modération ; qu'ainsi les contributions transmises, susceptibles d'engager la responsabilité civile et pénale du ministère ne sont pas diffusées par le modérateur ; qu'en particulier une contribution contenant des informations relatives à un tiers, de nature à porter atteinte à sa considération ou à l'intimité de sa vie privée, ne sera pas mise à la disposition du public ; que, de plus, afin d'empêcher la diffusion d'informations pouvant porter préjudice à un tiers dont l'identité aurait été usurpée ou l'intitulé de l'adresse électronique (e-mail) communiquée à son insu, il sera procédé, en cas de doute, à la vérification des informations auprès de la personne concernée avant diffusion de la contribution ;

Considérant que les utilisateurs du site accédant au forum sont informés de sa finalité, de ses règles de fonctionnement ainsi que des mentions prévues à l'article 27 de la loi du 6 janvier 1978 ;

Considérant que la durée de conservation des contributions émises dans le cadre du forum ne dépasse pas celle de l'inscription du thème du débat concerné ;

Considérant que les utilisateurs du site ont la possibilité de transmettre un courrier au ministre ou à ses services au moyen d'une boîte aux lettres ; qu'ils sont avertis dès la page d'accueil du service des risques relatifs au secret des correspondances transmises sur Internet vers le site et qu'en conséquence il leur est conseillé de ne pas utiliser ce service pour des courriers de nature personnelle ;

Considérant que les personnes sont avisées qu'elles peuvent, si elles le souhaitent, accompagner le message qu'elles transmettent de leur nom, de leur adresse de domicile, de leur adresse électronique, du nom de l'organisme au titre duquel elles adressent leur message, leur fonction, le motif et le sujet du message, leur catégorie socioprofessionnelle ; qu'il est explicitement indiqué que ces informations sont collectées de manière facultative ;

Considérant que les courriers ainsi recueillis sont transmis au service du ministère en charge du site qui le traite de la même manière que le courrier postal ; que des réponses à caractère administratif pourront être faites par la voie du courrier électronique ; qu'en revanche, les réponses personnalisées ne pourront être faites que par la voie postale ;

Considérant que le site comporte également un espace destiné aux jeunes afin de les familiariser avec les services Internet publics ; que cet espace comporte la possibilité de transmettre un message au ministre au moyen d'une boîte aux lettres spécifique, ainsi que de participer à des concours ;

Considérant que les utilisateurs de ces deux services sont susceptibles d'être des mineurs ; qu'en conséquence il leur est proposé de n'accompagner leur message, et de manière facultative, que de leur prénom ou d'un pseudonyme, de leur commune et pays de résidence, de leur âge et de leur classe ; qu'ils sont informés qu'aux fins de participer effectivement à un concours ils doivent en outre, avec l'accord de leurs parents, adresser leur réponse par courrier postal ;

Considérant qu'au-delà des mesures précitées destinées à garantir les droits des personnes, des mesures de sécurité offrant des garanties d'efficacité sont prises, notamment en vue d'empêcher des accès au site de nature à porter atteinte à l'intégrité des informations mises à la disposition du public ainsi qu'au détournement de finalité des informations recueillies sur le site ;

Considérant que la mise en oeuvre des procédures de sécurité repose en particulier sur l'examen périodique des fichiers des connexions des utilisateurs au site ; que dans ces fichiers peuvent être conservés, au fur et à mesure des connexions des utilisateurs, notamment leur adresse Internet (adresse IP) ou celle de la machine à laquelle ils se connectent, le nom de domaine, la requête (page consultée, par exemple), la date et l'heure de la requête ;

Considérant que ces informations ne sont accessibles qu'au seul responsable de la sécurité ; que la durée de conservation de ces informations, fixée à quinze jours, est strictement limitée à la durée nécessaire pour assurer la sécurité du site ;

Considérant, en outre, que pourront être exploitées à des fins statistiques les données relatives au pays de localisation de la machine ayant établi une connexion, à la date et l'heure de la connexion et à la nature de la requête ;

Considérant que le contrat de sous-traitance, en cas d'hébergement du site, interdira au sous-traitant toute cession, vente, location ou exploitation des fichiers log ou autres traces de connexion ;

Considérant que préalablement à la mise en oeuvre d'un site ministériel sur Internet, le ministre concerné devra adresser à la Commission une déclara-

tion de conformité faisant référence au présent modèle type ; que cette déclaration de conformité devra comporter l'indication des services assurés par le site, les informations nominatives correspondant à ces services, le lieu d'exercice du droit d'accès et une annexe précisant les procédures de sécurité mises en œuvre pour ce site ;

Émet un avis favorable au projet d'arrêté du Premier ministre portant modèle type de traitements d'informations nominatives mis en œuvre dans le cadre d'un site Internet ministériel.

B. Le site de la ville de Paris

À l'instar des sites institutionnels ouverts par les administrations centrales, de nombreuses villes souhaitent se doter de leurs propres sites. Ainsi, le maire de Paris a saisi la CNIL de son projet de diffuser sur Internet des informations sur les services de la Ville de Paris et d'ouvrir un service de messagerie électronique.

Les informations nominatives diffusées sur ce site concernent d'une part, les élus (maire, conseillers, adjoints...), d'autre part, les directeurs des services de la ville et du département de Paris et diverses personnalités (chefs d'État reçus à l'Hôtel de Ville, lauréats de concours organisés par la ville). À cet égard, et conformément à la doctrine de la CNIL, la mairie de Paris s'est engagée à informer par écrit les personnes concernées sur les risques de captation, de déformation et de détournement de finalité inhérents au réseau Internet, afin qu'elles puissent le cas échéant exercer leur droit d'opposition.

Les données relatives aux élus, à leurs adjoints, aux conseillers de Paris, aux conseillers d'arrondissement et aux directeurs des services de la ville de Paris sont conservées pendant la durée de leur mandat ou de leurs fonctions.

Cependant, à la demande de CNIL, la mairie de Paris a réduit de six mois à deux semaines, la durée de conservation des données relatives aux connexions des visiteurs du site : cette durée paraît en effet suffisante à la CNIL, qui a consulté sur ce point le service central de la sécurité des systèmes d'Information (SCSSI), pour assurer la sécurité du site.

De même, la mairie de Paris, qui souhaitait conserver les données relatives aux courriers électroniques pendant un délai d'un mois dans la messagerie électronique du site et pendant six mois sur disquette informatique, a accepté de se limiter à la sauvegarde mensuelle sur le site, conformément aux recommandations de la Commission.

Par ailleurs, la CNIL a pris acte de ce que les modalités de traitement des courriers électroniques adressés par les internautes seront conformes aux règles de répartition des compétences entre la mairie de Paris et les mairies d'arrondissement de sorte qu'en aucun cas l'existence même du site puisse aboutir à modifier les règles de répartition des compétences. Dans ces conditions, un avis favorable a été rendu sur la demande d'avis relatif au site Internet de la ville de Paris.

Délibération n° 97-051 du 30 juin 1997 concernant une demande d'avis présentée par la mairie de Paris relative à un traitement d'informations nominatives mis en œuvre dans le cadre du site Internet de la Ville de Paris

(Demande d'avis n° 517 197)

La Commission nationale de l'informatique et des libertés,

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

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

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ; Vu le code général des collectivités territoriales ; Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ; Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ;

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation de télécommunications ; Après avoir entendu Monsieur Marcel Pinet, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ; Considérant que la Commission a été saisie par la mairie de Paris d'une demande d'avis relative à un traitement d'informations nominatives mis en œuvre dans le cadre du site Internet de la Ville de Paris ; que ce site a pour objet de diffuser des informations sur la Ville de Paris en tant que capitale touristique, économique et universitaire et, au titre de la communication municipale, de diffuser des informations sur les services de la ville et du département ; qu'en outre, un service de messagerie électronique permettra aux utilisateurs du site d'adresser des courriers électroniques ; Considérant que les informations nominatives diffusées sur le site concernent, d'une part, les élus, c'est-à-dire le maire, les conseillers de Paris, les adjoints au maire de Paris, les maires d'arrondissements, les conseillers d'arrondissements, d'autre part, les directeurs des services de la Ville de Paris et du département de Paris, enfin, des personnalités, qu'il s'agisse des chefs d'États ou autres personnages publics reçus à l'Hôtel de Ville, ainsi que les personnes citées dans le cadre des rubriques du site et les lauréats de concours ou d'épreuves organisés ou parrainés par la Ville de Paris ; Considérant que les catégories d'informations traitées et diffusées sont, pour le maire, l'identité, la vie professionnelle et la vie politique, les publications, et pour les autres personnes concernées, l'identité et, le cas échéant, le titre, la fonction, les attributions, l'organisme, l'arrondissement d'élection, ou, pour les lauréats de concours ou d'épreuves organisés ou parrainés par la Ville de Paris, l'âge ;

Considérant que les conseillers de Paris, les conseillers d'arrondissements et les directeurs de services de la Ville de Paris sont informés par voie de notes d'information, préalablement à la diffusion sur le site Internet de la Ville de Paris de données les concernant, des risques de captation, de déformation et de détournement de finalité inhérents au réseau Internet et de leur droit de s'opposer, préalablement et à tout moment, à cette

diffusion ; que les personnes sont également informées des droits dont elles disposent en application des articles 27 et 34 de la loi du 6 janvier 1978 ; qu'il convient sur ce point que le projet de note d'information adressé aux personnes concernées soit complété, à la première phrase du sixième paragraphe, afin de préciser la nature des risques inhérents au réseau Internet ; qu'ainsi, il convient d'ajouter après les mots « inhérents à ce mode de diffusion », les mots « (intrusion, falsification, divulgation) » ;

Considérant qu'il convient qu'une information de même nature puisse être fournie, selon des modalités appropriées, aux personnalités reçues à l'Hôtel de Ville, ainsi qu'aux personnes citées dans le cadre des rubriques du site ; que, s'agissant des lauréats de concours, la mairie de Paris s'engage à faire figurer sur l'acte de participation à ces concours une mention indiquant que les lauréats pourront voir leur nom être diffusé sur Internet et les informant de leur droit d'opposition ; que dans le cas particulier des lauréats mineurs, la diffusion sera subordonnée à l'accord des parents ;

Considérant que les données relatives aux élus, à leurs adjoints, aux conseillers de Paris, aux conseillers d'arrondissements et aux directeurs des services de la Ville de Paris sont conservées pendant la durée des fonctions dévolues à ces personnes ; que les courriers électroniques adressés par les utilisateurs du site ne sont conservés sur support informatique que pendant un délai d'un mois ;

Considérant, en outre, que les données relatives aux connexions opérées par les visiteurs du site sont conservées à des fins de sécurité et d'établissement de statistiques de consultation pendant un délai de deux semaines ;

Considérant que les informations traitées par le service de messagerie électronique au site sont le contenu du courrier électronique et, le cas échéant, l'identité, l'adresse, l'organisme ou la société et les moyens de communications (téléphone, télécopie, e-mail) indiqués par la personne qui a adressé un courrier électronique ; qu'une mention apparaissant à l'écran rappellera aux utilisateurs du site que la confidentialité des informations circulant sur le réseau Internet n'est pas garantie ;

Considérant que les destinataires des informations nominatives relatives aux personnes qui adressent un courrier électronique à la messagerie électronique du site sont la direction générale de l'information et de la communication de la Ville de Paris et, le cas échéant, la direction, l'élu ou le conseil concerné par le message électronique ;

Considérant que les courriers électroniques, au même titre que toutes les correspondances reçues par la mairie de Paris, seront adressés sous forme d'une édition papier intégrale, aux directions, aux élus, ou aux conseils, lorsque ces courriers leur seront destinés nommément ou es-qualité ;

Considérant, en outre, qu'à défaut de l'indication par l'utilisateur d'un destinataire, les courriers électroniques seront adressés sous forme d'une édition papier intégrale, à l'élu ou au conseil légalement compétent pour y répondre ; qu'à cet égard, la Commission prend acte que les modalités de traitement des courriers électroniques adressés par les utilisateurs du site Internet de la Ville de Paris seront conformes aux règles de répartition des compétences entre la mairie de Paris et les mairies d'arrondissements ;

Émet un avis favorable **au projet d'arrêté du maire de Paris.**

C. La simplification des formalités administratives

La volonté du Gouvernement de rendre l'administration accessible par voie électronique ne s'exprime pas seulement dans la diffusion de données publiques sur le réseau Internet. La dématérialisation de procédures administratives et le développement des téléprocédures en constitue le deuxième volet. Le plan d'action gouvernemental rendu public le 16 janvier 1998 prévoit notamment que l'ensemble des formulaires administratifs devra être disponible sur Internet avant la fin de 1998. Chaque internaute pourra alors télécharger les documents et les imprimer, sans avoir à les solliciter par courrier ou en se déplaçant à un guichet. Lors de cette première étape, les documents dûment remplis seront adressés à l'administration concernée par courrier et non par Internet. Dans une deuxième étape, les formulaires pourront être remplis en ligne. La commodité qui en résultera ne pourra être réalisée que lorsque des mesures de sécurité appropriées et aisées à mettre en oeuvre seront réunies. Certaines expérimentations sont cependant actuellement en cours et suivies par la CNIL avec la plus grande attention.

Dans ce contexte, la CNIL a été saisie par la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) d'une demande d'expérimentation pendant six mois d'une procédure de transmission par Internet des déclarations de données sociales que les entreprises sont tenues d'effectuer auprès du centre de transfert de données sociales. Ce système de télédéclaration administrative par le réseau, qui a été le premier du genre à être présenté à la CNIL, vise donc à l'allégement des formalités administratives et devrait être suivi de nombreux autres.

Compte tenu des risques inhérents à l'utilisation d'Internet et du caractère nominatif des données transmises dans la déclaration annuelle de données sociales des entreprises, la CNAVTS s'est montée très attentive à la question de la sécurité. Ainsi, les données font l'objet d'un chiffrement avec utilisation d'un protocole autorisé par le service central de la sécurité des systèmes d'information (SCSSI).

La Commission a donné un avis favorable à la mise en oeuvre de cette expérimentation, en demandant à la CNAVTS de lui en transmettre le bilan. Toutefois, dans l'hypothèse d'une généralisation du système, les mesures de sécurité devraient être réexaminées.

Délibération n° 97-017 du 11 mars 1997 portant avis sur la demande présentée par la caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) et concernant une expérimentation de transfert de données sociales par le réseau Internet (TDS-INTERNET)

(Demande d'avis n° 492 532)

La Commission nationale de l'informatique et des libertés,

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 le décret n° 85-1343 du 16 décembre 1985 modifié instituant un système de transfert de données sociales ;

Vu les délibérations n° 84-27 du 26 juin 1984, 85-34 du 9 juillet 1985, 88-27 du 8 mars 1988, 92-048 du 21 avril 1992, 93-057 du 6 juillet 1993 et 94-023 du 29 mars 1994 relatives au transfert des données sociales ; Vu le projet d'acte réglementaire présenté par la caisse nationale d'assurance vieillesse des travailleurs salariés ;

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

Considérant que la caisse nationale d'assurance vieillesse des travailleurs salariés a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis portant sur la transmission, à titre expérimental, par le moyen du réseau Internet, des déclarations annuelles de données sociales établies par les employeurs ; que l'expérimentation consiste en un traitement fictif des données sociales portant sur l'année 1996 ; que cette expérimentation a pour seul objet de tester la faisabilité de ce mode de transmission de données entre les entreprises et leur interlocuteur unique, le centre de transfert de données sociales ; que, pour l'expérimentation, seules seront concernées cinq à dix entreprises volontaires, ainsi que les services de la caisse nationale d'assurance vieillesse des travailleurs salariés ; Considérant que les données transmises ne seront conservées sur des fichiers spécifiques que pendant la durée de l'expérimentation, soit pendant six mois ; Considérant qu'eu égard au caractère confidentiel des informations traitées, la caisse nationale d'assurance vieillesse des travailleurs salariés a pris un certain nombre de précautions afin d'assurer la sécurité des données transmises sur le réseau Internet ; qu'ainsi, en particulier, une procédure d'authentification entre les sites, de chiffrement des données et de signature électronique est destinée à éviter que les données transférées ne soient déformées, endommagées ou communiquées à des tiers non autorisés ; que ce protocole sécurisé dénommé SSL a été autorisé par le service central de la sécurité des systèmes d'information (SCSSI) ;

Considérant que la protection du site central de la caisse nationale d'assurance vieillesse des travailleurs salariés est assurée par un dispositif de filtrage, de type pare-feu, destiné à garantir l'accès contre les risques d'intrusion sur le réseau ;

Considérant que les mesures de sécurité adoptées sont satisfaisantes ; Considérant qu'il apparaît nécessaire que les salariés des entreprises concernées par l'expérimentation soient informés de sa mise en place et des droits qui leur sont reconnus par la loi du 6 janvier 1978 ;

Émet *un* avis favorable au projet d'acte réglementaire présenté par la caisse nationale d'assurance vieillesse des travailleurs salariés décidant de la mise en place d'une expérimentation limitée à six mois destinée à évaluer la fiabilité des transmissions des déclarations annuelles de données sociales par le moyen du réseau Internet,

Demande à être destinataire du bilan de l'expérimentation.

II. PATIENTS ET DEMANDEURS D'EMPLOIS SUR LE RÉSEAU

A. Des informations particulièrement protégées : les données de santé

L'informatique constitue on le sait une des clés de voûte de la réforme du système de santé engagée par les pouvoirs publics depuis plusieurs années et consacrée par l'ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de santé. En effet, ce texte prévoit notamment la généralisation des cartes de santé, le développement des réseaux et des systèmes d'information de l'assurance maladie, l'informatisation des professions de santé et l'expérimentation de réseaux de soins.

L'informatisation du secteur santé nécessite sans aucun doute une vigilance particulière : d'abord parce qu'il représente un gisement d'informations considérable ; ensuite parce que ce secteur revêt un aspect très hétérogène (1060 hôpitaux publics, 460 hôpitaux privés gérant un service public, 3000 cliniques privées, 300 000 professionnels de santé, 4 000 laboratoires d'analyses, 6 000 pharmacies et toutes les caisses de sécurité sociale) ; enfin par les enjeux économiques, financiers et commerciaux dont il est l'objet (le marché des nouvelles technologies du secteur de la santé représenterait actuellement plus de 5 milliards de francs et dépasserait rapidement les 10 milliards). S'agissant de la protection des données personnelles, la CNIL suit avec beaucoup d'attention les effets de la multiplication des fichiers informatiques et de la circulation accrue des informations médicales à caractère personnel qui va résulter du dispositif « SESAM-VITALE », lequel repose sur la dématérialisation des feuilles de soins, la diffusion de cartes électroniques individuelles aux bénéficiaires de l'assurance maladie et l'informatisation d'une partie de l'activité des professionnels de santé (cf. *infra* 3^{e} partie, chapitre 7).

Par ailleurs, la Commission demeure particulièrement attentive aux conséquences de la médicalisation des systèmes d'information de l'assurance maladie qui va accompagner l'informatisation massive des secteurs de la santé et de la protection sociale. Ainsi, la Commission a-t-elle à plusieurs reprises rappelé que l'obligation faite aux professionnels de santé, de transmettre, sous forme nominative, aux caisses d'assurance maladie le code détaillé des prestations délivrées, des actes pratiqués ainsi que des pathologies diagnostiquées, nécessitait la recherche d'un juste équilibre entre les impératifs de maîtrise des dépenses de santé et la préservation des droits des personnes. À cet égard, dès 1995, la CNIL avait demandé, lors de l'examen du dispositif du codage des actes de biologie, que la CNAMTS procède à une évaluation des systèmes de sécurité et des modalités de chiffrement des données mis en oeuvre pour protéger les télétransmissions des données nominatives associées au code des actes.

D'une façon générale, la mise en place de réseaux de transmission d'informations médicales nominatives entre des partenaires variés (médecins,

caisses de sécurité sociale, organismes de recherche médicale...) constitue une des préoccupations majeures de la CNIL, en particulier dans la perspective du recours à un réseau ouvert tel qu'Internet, dont la CNIL a déjà souligné les risques actuels. En effet, les facilités d'intrusion dans les systèmes informatiques internes et les risques de divulgation et de déformation des informations ne sont pas négligeables, alors même que les données de santé sont désormais convoitées, à des fins marchandes, ce qui ne peut qu'accroître les risques de détournement et d'atteinte à la vie privée des personnes. Aussi, lorsqu'elle a été saisie des premières applications de transfert sur Internet de données médicales, notamment par l'agence nationale de recherche sur le sida dans le cadre d'une collaboration avec un institut de recherche britannique, la CNIL, tout en prenant acte que seules seront transmises des données codées ne comportant pas les noms des patients, a toutefois demandé le recours à un serveur spécifique pour le transfert des données et l'instauration de protections logicielles (cf. 17^{e} rapport, p. 83).

Parallèlement, la multiplication des télétransmissions d'informations médicales crée par elle-même un marché des données de santé qui donne un relief particulier aux questions de protection des données et de la vie privée. En effet, la Commission constate l'apparition de procédés visant à collecter auprès des professionnels de santé, des informations plus ou moins individualisées sur leurs prescriptions et leurs pratiques médicales, afin d'en assurer, de façon centralisée, l'exploitation statistique, notamment à des fins commerciales. Ces systèmes d'informations médicales, conçus généralement par des sociétés de communication médicale pour le compte de certaines filiales de laboratoires pharmaceutiques, ainsi que par des syndicats de professionnels de santé, reposent sur la mise à disposition des professionnels de santé d'un réseau, et parfois d'équipements informatiques, qui permettent de gérer les dossiers médicaux et de télétransmettre les données de prescriptions. Ainsi l'industrie pharmaceutique, par exemple, peut-elle détenir des gisements considérables d'informations pouvant lui permettre d'orienter les actions de publicité pour des médicaments. Dans le même temps, les professionnels de santé peuvent avoir intérêt à disposer de cette information, autant dans le souci de cerner leur propre activité que de posséder des indicateurs sur les comportements et les pratiques médicales. À cet égard, la CNIL veille à ce que ces systèmes d'information médicale soient mis en place dans des conditions respectant tant les règles de protection des données que les dispositions du code de la santé publique qui proscrivent formellement l'utilisation commerciale des données de prescription dès lors que les informations exploitées sont susceptibles de permettre l'identification des prescripteurs (cf. 16^{e} rapport, p. 108 et 17^{e} rapport, p. 232).

Dans cette conjoncture de croissance exponentielle des échanges d'informations nominatives dans le domaine de la santé, la CNIL s'efforce de concilier le respect de la confidentialité des données personnelles, c'est-à-dire du secret médical et de la vie privée, et la nécessaire circulation des informations. Dans cet esprit, et après concertation avec le Conseil national de l'Ordre des médecins, la CNIL a adopté, le 4 février 1997, une recommandation de

portée générale sur le traitement de données de santé à caractère personnel, visant à rappeler aux différents acteurs du système de soins les règles à respecter en matière d'informatique, de libertés et de santé, notamment au regard des risques de dérives commerciales *[journal officiel du* 12 avril 1997).

Conformément aux principes fondamentaux régissant le système de soins en France, en particulier le respect de l'intimité de la vie privée et de la liberté des personnes, le secret professionnel, l'indépendance professionnelle et morale des médecins, la Commission a rappelé que les données de santé ne peuvent être utilisées que dans l'intérêt direct du patient, et dès lors, leur exploitation à des fins commerciales est proscrite, de même que celle des informations sur les professionnels de santé, en particulier celles relatives à la nature de leurs prescriptions.

La CNIL a également appelé l'attention des professionnels de santé sur la nécessité de garantir l'anonymat des patients lors de transmissions de données vers un système d'information médicale ; par conséquent, le professionnel de santé adhérant à un tel système doit non seulement s'assurer de l'anonymat des données relatives à ses patients, mais s'entourer aussi de garanties contractuelles avec l'organisme responsable du système d'information afin de préserver cet anonymat.

Enfin, pour éviter tout risque de divulgation et d'utilisation détournée des informations, la Commission a recommandé que les données nominatives soient chiffrées et que toute mesure soit prise afin d'éviter, en cas de réseau privé, tout accès incontrôlé ou toute connexion à un réseau ouvert. Ainsi, dans le domaine de la santé, seules des messageries professionnelles sécurisées et recourant au chiffrement des données peuvent être utilisées pour transférer des données médicales nominatives.

Délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et notamment son article 6 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et notamment ses articles 6, 19 et 29 ;

Vu la loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu les articles 226-13 et 226-14 du code pénal relatifs au secret professionnel ; Vu le code de la santé publique et notamment ses articles L. *55*1 et suivants, L. 365-1 et L. 365-2 ; Vu le code de la sécurité sociale et notamment l'article L. 161-29 ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi du 6 janvier 1978 et notamment son article premier ;

Vu le décret n° 95-100 du 6 septembre 1995 portant code de déontologie médicale et notamment ses articles 4, 5, 12, 19, 20, 23, 24, 45, 73 et 91 ;

Après avoir consulté le Conseil national de l'Ordre des médecins ;

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

Constatant que le développement, dans le domaine de la santé, des technologies de l'information et, en particulier, des réseaux de communication ainsi que l'application des mesures de maîtrise des dépenses de santé, définies par les pouvoirs publics, favorisent la mise en place, sur initiative privée, de systèmes d'informations médicales, fondés sur le recueil, auprès des professionnels de santé, de données individualisées relatives à leurs prescriptions et à leur pratique médicale ; que ces données sont susceptibles d'être traitées, notamment, de façon à :
- disposer, à des fins de connaissance, d'évaluation et d'utilisation commerciale, d'informations sur l'activité médicale, destinées d'une part, aux instances représentatives des professions de santé ainsi que, le cas échéant, aux autres partenaires institutionnels du système de santé et d'autre part, aux sociétés de communication médicale et aux laboratoires pharma ceutiques pour leur permettre notamment de réaliser, auprès des profession nels de santé, des actions d'information et de publicité pour les médicaments ;
- permettre aux professionnels de santé, fournisseurs des données, de disposer d'informations statistiques sur leur propre activité ainsi que, le cas échéant, d'outils informatiques d'aide à la gestion du cabinet ou de systèmes d'aide à la décision ;
- expérimenter une nouvelle forme d'organisation du système de santé fondée sur la mise en place de réseaux de soins, prévue par l'article L. 162-31-1 du code de la sécurité sociale.

Considérant que les données traitées sont susceptibles d'être recueillies selon des modalités différentes, telles que :
- les enquêtes sur les habitudes de prescription réalisées par voie de questionnaires auprès d'un échantillon représentatif de professionnels consti tué à partir des fichiers nominatifs dont disposent les laboratoires pharma ceutiques et les sociétés de communication médicale ;
- les télétransmissions périodiques, par les médecins, d'informations ex traites des fichiers médicaux gérés sur des équipements informatiques et à partir de logiciels mis à la disposition des professionnels de santé ;
- l'utilisation, selon des modalités techniques particulières, des télétrans missions de données de facturation, réalisées dans le cadre de la délégation de paiement (tiers-payant) vers les caisses d'assurance maladie, via le plus souvent des organismes intermédiaires, pour certains, gérés par la profes sion de santé considérée ;

Constatant que le développement de ces systèmes d'information, en raison des finalités poursuivies et des modalités de collecte des données, est susceptible d'avoir des conséquences importantes sur les principes fondamentaux qui régissent aujourd'hui le système de soins en France et en particulier sur le respect de l'intimité de la vie privée et de la liberté des

personnes, sur le secret professionnel et sur l'indépendance professionnelle et morale des médecins ;

Considérant que la collecte et le traitement de données, qui sont directement ou indirectement nominatives à l'égard du patient ou du professionnel de santé concerné, doivent respecter les dispositions protectrices de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et doivent en particulier, faire l'objet de formalités préalables auprès de la CNIL ; qu'ainsi la Commission a été saisie, par des sociétés de communication médicale, pour certaines filiales de laboratoires pharmaceutiques, et par des syndicats de professionnels de santé, de déclarations relatives à la mise en œuvre de tels systèmes ;

Estime qu'il y a lieu, dans le contexte actuel, de rappeler et de préciser, par la présente recommandation, les garanties à respecter lors du traitement et de la transmission des données à caractère personnel relatives à la santé ;

Considérant que la connaissance de l'état de santé d'une personne constitue une information qui relève de l'intimité de sa vie privée et qui est protégée par le secret médical ; en conséquence, le traitement de cette information nécessite, conformément à l'article 6 de la Convention n° 108 du Conseil de l'Europe susvisée, l'adoption de garanties appropriées ;

Rappelle que les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et, dans les conditions déterminées par la loi, pour les besoins de la santé publique et que, dès lors leur exploitation à des fins commerciales doit être proscrite. En conséquence, ces données ne peuvent être traitées que dans le respect des droits des personnes et des règles déontologiques en vigueur.

Recommande, en conséquence, le respect des principes suivants :

Sur l'utilisation des données de santé à caractère personnel

La Commission estime qu'il y a lieu de rappeler que :
— conformément aux articles 226-13 et 226-14 du code pénal, la révéla tion d'informations à caractère secret par une personne qui en est déposi taire, soit par état soit par profession, hormis les cas où la loi l'impose ou l'autorise, est passible de sanctions pénales ;
— en application de l'article L. 365-2 du code de la santé publique, sont interdites, sous peine de sanctions pénales, « la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'arti cle L. 161-29 du code de la sécurité sociale, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel pre scripteur » ;
— conformément à l'article L. 365-1 du code de la santé publique, « est interdit le fait, pour les membres des professions médicales, de recevoir des avantages en nature ou en espèces, sous quelque forme que ce soit, d'une façon directe ou indirecte, procurés par des entreprises assurant des presta tions, produisant ou commercialisant des produits pris en charge par les régimes obligatoires de sécurité sociale » ;
— aux termes de l'article 25 de la loi du 6 janvier 1978, la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite.

La Commission considère que, au sens de l'article 5 de la Convention n° 108 du Conseil de l'Europe, le traitement de données de santé à caractère personnel est légitime dès lors qu'il a pour finalités de permettre au professionnel de santé de mieux assurer le suivi médical des patients, de faciliter leur prise en charge par les organismes d'assurance maladie obligatoire, de participer aux actions de prévention et de veille sanitaire poursuivies par les autorités de santé et de contribuer aux travaux de recherche médicale. Dans le cadre de ces finalités, les données de santé à caractère personnel, dont l'usage est en principe réservé au professionnel de santé qui a procédé au recueil de ces données, peuvent être communiquées sous certaines conditions à des destinataires et tiers habilités à en connaître en vertu de la loi.

Les professionnels de santé sont ainsi tenus, (articles 226-14 du code pénal, articles L. 11 et suivants du code de la santé publique...) de déclarer aux autorités judiciaires, médicales ou administratives, certains situations dont ils ont connaissance.

En outre, conformément au code de la sécurité sociale et notamment à l'article L. 161-29, dans l'intérêt de la santé publique et en vue de contribuer à la maîtrise des dépenses d'assurance maladie, les professionnels et les organismes ou établissements dispensant des actes ou prestations remboursables par l'assurance maladie à des assurés sociaux ou leurs ayants droit sont tenus de communiquer aux organismes d'assurance maladie concernés le numéro de code des actes effectués, des prestations servies à ces assurés sociaux et à leurs ayants droit et des pathologies diagnostiquées.

Ces données sont également susceptibles d'être communiquées, sous forme anonyme, aux unions professionnelles instituées par la loi du 18 janvier 1994.

Les professionnels de santé peuvent également transmettre à des fins statistiques, dans les conditions prévues par la loi du 1er juillet 1994, des données médicales nominatives issues de leur activité à des organismes autorisés à mettre en œuvre, à des fins de recherche médicale, des traitements de données de santé à caractère personnel.

Enfin, conformément à l'article 45 du code de déontologie médicale, le médecin, à la demande du patient ou avec son consentement, peut transmettre aux médecins qui participent à la prise en charge de ce patient ou à ceux qu'il entend consulter, les informations et documents utiles à la continuité des soins.

La Commission rappelle en conséquence que :

- hors les cas prévus par la loi, les professionnels de santé ne peuvent transmettre à des tiers, les données de santé à caractère personnel relatives à leurs patients, sans qu'au préalable ces données aient été rendues anonymes ;
- conformément à l'article L365.2 du code de la santé publique et à l'application qu'entend en faire le ministère en charge de la Santé, ces données, même rendues anonymes à l'égard des patients, ne peuvent être utilisées à des fins de promotion ou de prospection commerciale, dès lors qu'elles sont associées à l'identification du professionnel de santé.

La Commission recommande que, conformément aux articles L. 462 et L. 365-1 du code de la santé publique, les instances ordinales concernées soient consultées lors de la mise en place de systèmes d'informations médicales, en particulier, sur les modalités de participation des professionnels de santé.

Sur l'information et le respect des droits des personnes

La Commission recommande que les professionnels de santé susceptibles de participer à des systèmes d'informations médicales et de transmettre sous quelque forme que ce soit des données, soient clairement informés de l'identité du ou des organismes juridiquement responsables du système, de ses finalités, des conséquences à leur égard de leur participation, des destinataires des informations transmises, des modalités d'exercice de leur droit d'accès, de rectification et de suppression. Dans les cas où l'organisme tiers mettrait à la disposition du professionnel de santé des moyens informatiques lui permettant de gérer ses dossiers médicaux, il importe que les modalités de cette mise à disposition lui soient clairement précisées et qu'il conserve, quelles que soient les modalités de communication des informations issues de son fichier, la maîtrise de cette communication.

Ainsi, en cas d'abandon de collaboration, l'organisme tiers devrait s'engager à fournir au professionnel de santé les moyens nécessaires pour lui permettre de continuer à gérer sur informatique ses dossiers médicaux ou d'effacer les informations nominatives enregistrées avant restitution du matériel informatique à l'organisme.

La Commission estime également que, pour garantir une information claire et complète des professionnels de santé, il importe que les contrats conclus entre les organismes tiers et les professionnels de santé fassent expressément mention des points précités.

Elle recommande également que, nonobstant les dispositions prises pour assurer l'anonymat des patients, les organismes tiers destinataires des informations issues des fichiers médicaux s'engagent vis-à-vis des professionnels de santé, à prendre toutes précautions utiles afin d'éviter la déformation, la divulgation ou l'utilisation détournée des données issues directement ou non des prescriptions médicales, dès lors que ces données permettent l'identification des professionnels de santé. De plus, il importe de rappeler que les professionnels de santé ne peuvent transmettre que des données concernant leur propre activité, à l'exclusion donc de toute information concernant ou provenant d'un autre confrère ou d'un autre professionnel de santé.

Il convient en outre de rappeler que, dans les cas où la loi impose ou autorise la transmission des données médicales directement ou indirectement nominatives concernant leurs patients à des organismes tiers dûment habilités à en connaître, les professionnels de santé doivent en **informer** leurs patients de façon à ce qu'ils puissent exercer les droits qui leur sont reconnus par la loi du 6 janvier 1978. Ainsi, hors les cas où la transmission est imposée par la loi, les patients doivent pouvoir s'opposer aux communications d'informations les concernant.

Sur le respect de la confidentialité des informations et la sécurité des traitements

La Commission estime qu'il y a lieu de rappeler qu'en application des articles 29 et 45 alinéa 1 de la loi du 6 janvier 1978, les professionnels de santé s'engagent, vis-à-vis des patients, à prendre toutes précautions utiles afin de préserver la sécurité des informations relatives à leur état de santé et notamment d'empêcher qu'elles ne soient déformées ou communiquées à des tiers non autorisés. Le non respect de cette disposition est passible des

sanctions pénales prévues au titre de l'article 226-17 du code pénal. Enfin, il convient de noter qu'en vertu de l'article 45 du décret du 6 septembre 1995, portant code de déontologie médicale, les dossiers médicaux des patients doivent être conservés sous la responsabilité des médecins qui en assurent le suivi.

La Commission recommande donc que, préalablement à toute transmission, aux systèmes d'information médicale précédemment visés, de données issues de leur activité, les professionnels de santé s'assurent du respect effectif de l'anonymat des données relatives à leurs patients et que les organismes tiers, destinataires des données s'engagent, par voie contractuelle, vis-à-vis des professionnels de santé, à prendre les dispositions nécessaires pour garantir et maintenir cet anonymat, notamment lors du traitement ultérieur de ces données. Ainsi, en cas de télétransmission, les professionnels de santé doivent pouvoir disposer des moyens techniques nécessaires pour vérifier ou faire vérifier que les dispositifs adoptés garantissent effectivement l'anonymat des données concernant les patients.

La Commission rappelle qu'elle peut, dans le cadre des missions de contrôle qui lui sont confiées par l'article 21, 2 de la loi du 6 janvier 1978, procéder, à l'égard de tout traitement, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission.

Par ailleurs, il importe que dans les cas où il serait nécessaire pour l'organisme tiers de disposer, à des fins statistiques, de données de suivi individualisées [1] sur les patients, des procédures d'anonymisation reconnues et évaluées, reposant par exemple sur l'utilisation de techniques dites de « hachage » ou de chiffrement des données, puissent être retenues.

La Commission préconise que dans le cadre de l'expérimentation de filières ou de réseaux de soins faisant appel à des moyens informatiques, les transmissions de données nominatives éventuellement effectuées entre professionnels de santé soient réalisées dans des conditions garantissant de façon effective la confidentialité des données, et qu'en particulier il puisse être recouru, selon la sensibilité des données, au chiffrement de tout ou partie des données, dans le cadre de la réglementation française et européenne en vigueur.

Elle appelle également l'attention des professionnels de santé, de leurs instances représentatives, et de façon générale, des partenaires intéressés, sur les risques de divulgation et d'utilisation détournée des informations, inhérents à l'utilisation de réseaux de communication ouverts de type Internet et sur la nécessité de prendre des mesures de sécurité appropriées pour, d'une part, protéger les données nominatives par le chiffrement de celles-ci et d'autre part, en cas de réseau privé, restreindre effectivement l'accès de ce dernier aux seuls utilisateurs habilités et éviter tout accès incontrôlé sur le réseau ou une connexion à un réseau ouvert.

Enfin, la Commission préconise que, dans le domaine de la santé, seules des messageries professionnelles sécurisées et recourant au chiffrement des données puissent être utilisées pour transférer des données médicales nominatives.

[1] Au sens de la présente recommandation, sont considérées comme données de suivi individualisées, des informations qui peuvent être « chaînées » pour connaître l'évolution de l'état de santé d'une personne déterminée, sans que son identité soit connue de l'organisme tiers.

La Commission décide qu'il y a lieu en conséquence d'appeler l'attention tant des pouvoirs publics que des professionnels de santé et organismes intéressés sur les points précédemment évoqués.

À terme, l'ensemble de ces préconisations devrait permettre de prévenir les difficultés susceptibles de survenir à l'occasion de la mise en œuvre du réseau santé-social (RSS) dont les pouvoirs publics ont décidé la création pour parachever l'édifice informatique conçu pour le système de soins. En effet, la perspective de cet Intranet médico-social, qui devrait rapidement s'étendre à des applications de télémédecine, des systèmes de surveillance et d'alerte sanitaire, ou encore des réseaux d'épidémiologie, augmente les potentialités d'une commercialisation de données personnelles de santé.

Ainsi, l'annuaire des 300 000 professionnels de santé participant au réseau, accessoire indispensable qui sera disponible en ligne, représente une incontestable valeur marchande. Cet annuaire devrait en effet fournir, au minimum, l'adresse électronique d'un professionnel ou d'un service, à partir de plusieurs critères de recherche (nominatif, géographique ou thématique) et présenter ainsi un grand intérêt pour les opérateurs du marketing médical. D'ailleurs, le concessionnaire en charge du développement et de la maintenance de cet annuaire, pourra, dans un but de rentabilisation du réseau mais sous certaines conditions, procéder à la commercialisation de cet annuaire. La Commission s'attache sur ce point à ce que chaque professionnel de santé décide librement s'il autorise ou pas la cession à des fins commerciales des données le concernant figurant dans l'annuaire.

De surcroît, il convient de noter que le RSS ne disposant d'aucune exclusivité auprès des professionnels de soins, ces derniers pourront recourir aux services d'autres réseaux qui les connecteront aux points d'accès du RSS ; aussi, il apparaît nécessaire que les divers opérateurs intervenant à cette occasion soient soumis aux mêmes contraintes que celles imposées au RSS par le contrat de concession, en particulier au plan de la sécurité.

La CNIL a été conduite à préciser sa position sur les transmissions de données médicales nominatives par Internet, lors de l'examen des premières procédures de télémédecine par le réseau des réseaux. Ces expériences d'échanges de données entre hôpitaux et médecins de ville ont vocation à améliorer la prise en charge des patients en milieu extra-hospitalier, en facilitant la communication d'informations médicales entre les médecins participant au suivi des patients, et notamment celles des dossiers médicaux. À ce titre, les « réseaux ville-hôpital » s'inscrivent parfaitement dans la logique de coopération et de coordination entre les acteurs du système de soins, et répondent aux objectifs assignés aux réseaux de soins par l'ordonnance du 24 avril 1996 : favoriser la continuité des soins et promouvoir la délivrance de soins de proximité de qualité.

Le centre hospitalier d'Annecy a notamment présenté, à titre expérimental, un tel projet de télémédecine via Internet. Le réseau doit permettre au médecin hospitalier et au médecin de ville ayant en charge le patient, d'échan-

ger rapidement les informations médicales nécessaires au suivi de ce dernier, qu'il s'agisse de communiquer le compte rendu d'hospitalisation au médecin de ville ou, à l'inverse, de mettre à disposition du médecin hospitalier les informations nécessaires à la prise en charge médicale du patient lors de son hospitalisation. Une messagerie permettant des échanges d'informations professionnelles non nominatives entre les médecins est également mise en place.

La Commission relève le grand intérêt de tels échanges, sans ignorer le risque de divulgation et de déformation des données liés à l'utilisation d'Internet. Aussi, la CNIL n'a-t-elle délivré un avis favorable qu'après s'être assurée de l'efficacité des solutions de sécurité proposées. Aussi, après concertation avec le service central de la sécurité des systèmes d'information (SCSSI), compétent pour autoriser l'éventuel chiffrement des données, la CNIL a estimé que le recours à la cryptologie était indispensable pour assurer une protection efficace des données à caractère personnel circulant sur les réseaux. Il en résulte qu'il doit être procédé au chiffrement des données transmises par Internet, par un algorithme de cryptage autorisé par le SCSSI. De plus, un dispositif de filtrage des accès *(firewall)* doit être implanté pour éviter toute intrusion dans le système informatique interne de l'hôpital. Enfin, l'accès des médecins aux boîtes aux lettres électroniques doit être protégé par des procédures d'identification.

Il convient de noter qu'au début de l'année 1998, alors que la France disposait jusque là d'une réglementation généralement jugée contraignante en matière de chiffrement des données, le Gouvernement a publié les décrets d'application de la loi du 29 juillet 1996 sur les télécommunications, qui libéralise l'utilisation des procédés de cryptologie tout particulièrement celle du chiffrement dit « faible » (clés de moins de 40 bits).

À la lumière de ces évolutions dont on peut pressentir qu'elles vont modifier les relations entre les médecins et les patients, il convient sans doute de rappeler que les données médicales ne sont pas des données comme les autres ; la Convention 108 du Conseil de l'Europe de 1981 puis, plus récemment, la directive européenne du 24 octobre 1995 en ont fait une catégorie sensible, dotée d'une protection particulière, et chacun de nous comprend aisément le secret qui les entoure et la part d'intimité qu'elles renferment. Et la CNIL doit à cet égard continuer à faire en sorte que la technique demeure au service de l'éthique.

Délibération n° 97-049 du 24 juin 1997 portant avis sur la mise en œuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le centre hospitalier d'Annecy et certains médecins de ville

(Demande d'avis n° 453 828)

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 ;

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications et notamment son article 17 ;

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

Vu le décret n° 92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés ;

Vu le décret n° 95-1000 du 6 septembre 1995 portant code de déontologie médicale et, notamment son article 45 ;

Vu le projet d'acte réglementaire présenté par le centre hospitalier d'Annecy ;

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

Considérant que le centre hospitalier d'Annecy a saisi la Commission pour avis de la mise en oeuvre, pour une période d'expérimentation s'étendant jusqu'au 31 décembre 1998, d'un réseau de télémédecine entre des médecins de services hospitaliers et des médecins de ville volontaires ;

Considérant que ce réseau a pour finalité principale de faciliter, dans le cadre de la prise en charge des patients en milieu extra-hospitalier, la communication, entre les médecins précités, des informations médicales nominatives nécessaires au suivi de ces patients ; qu'il doit également permettre l'échange d'informations professionnelles non nominatives entre ces professionnels de santé ;

Considérant que l'utilisation par les médecins, de ce réseau, ne doit pas les exonérer de transmettre selon les voies habituelles les informations concernant les patients qu'ils suivent et, en particulier, le compte rendu d'hospitalisation ;

Considérant que cette application sera mise en oeuvre à partir de micro-ordinateurs reliés, en particulier, via le réseau Internet à un serveur de messagerie externe chargé d'assurer la gestion des boites aux lettres électroniques ;

Considérant que, compte tenu des risques de divulgation, de déformation et d'utilisation détournée des informations inhérentes au réseau Internet, le transfert par ce réseau de données médicales nominatives nécessite, conformément à l'article 6 de la Convention n° 108 du Conseil de l'Europe, l'adoption de garanties appropriées ;

Considérant à cet égard qu'il sera procédé au chiffrement des données échangées par ce réseau ainsi que des sauvegardes ; que ce chiffrement sera assuré par un moyen de cryptologie qui bénéficie d'une autorisation du service central de la sécurité des systèmes d'information dans la mesure où les clés de séquestre sont fournies par ce service ;

Considérant que cette solution peut être admise, à titre provisoire, en l'attente de la parution du décret qui, conformément aux dispositions de l'article 17 II de la loi du 26 juillet 1996, doit fixer les conditions dans lesquelles des organismes agréés pourront détenir les conventions secrètes des moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité ;

Considérant qu'il ne pourra être procédé au déchiffrement des données que par le médecin désigné comme destinataire de ces données ainsi que, le cas échéant, par l'autorité judiciaire, dans les conditions prévues à l'article 17 II de la loi du 26 juillet 1996 de réglementation des télécommunications ; que dans le cas précité, il serait souhaitable que le déchiffrement s'effectue qu'en présence d'un représentant du Conseil de l'Ordre ;

Considérant en outre, que l'accès aux boites aux lettres électroniques sera protégé par des procédures d'identification et d'authentification individuelle des utilisateurs ; qu'un dispositif de journalisation des connexions sera installé ; Considérant que pour éviter toute intrusion via le réseau Internet dans le système informatique du centre hospitalier, un dispositif de protection logiciel *(firewall)* sera installé pour filtrer les accès ; Considérant que ces mesures de sécurité apparaissent satisfaisantes ; Considérant que les patients seront informés par voie d'affichage et par les soins des médecins concernés, de la mise en place de ce réseau et des droits qui leur sont ouverts au titre des articles 34 et 40 de la loi du 6 janvier 1978 modifiée ; que le droit d'accès aux données conservées dans les fichiers médicaux constitués respectivement par les services hospitaliers et les médecins de ville pourra s'exercer auprès du médecin responsable du service dans lequel il aura été hospitalisé ainsi qu'auprès du médecin de ville assurant la prise en charge extra-hospitalière ; **Émet un avis favorable** au projet d'acte réglementaire du centre hospitalier d'Annecy portant expérimentation, jusqu'au 31 décembre 1998, du réseau de télémédecine.

B. Demandes d'emploi sur Internet

Plusieurs sociétés privées ont déclaré à la CNIL des serveurs d'annonces d'offres ou de demandes d'emploi, qui sont ouverts, sur abonnement, aux entreprises, aux cabinets de recrutement et aux personnes à la recherche d'un emploi (*cf.* 17e rapport, p. 89).

En 1997, c'est l'ANPE qui a ouvert, après avis favorable de la CNIL, un serveur expérimental d'offres et de demandes d'emploi. Ce site, expérimenté dans la région Nord-Pas-de-Calais, s'adresse exclusivement aux jeunes diplômés à la recherche d'un emploi et aux entreprises. Outre une présentation générale de l'ANPE, le serveur diffuse des offres d'emploi et des *curriculum vitae.* En fait, ce serveur s'inscrit dans le prolongement du traitement de l'ANPE dénommé « acte générique » qui a mis en œuvre de multiples outils de communication destinés à améliorer l'information des usagers et la régulation du marché de l'emploi (*cf.* 17e rapport, p. 351).

Concrètement, les personnes intéressées par une offre d'emploi peuvent, d'un « clic », obtenir l'adresse de l'employeur, de l'agence locale pour l'emploi ou du partenaire conventionné, si l'employeur a choisi de recevoir les réponses à ses offres par leur biais. Les entreprises intéressées par le CV d'un demandeur d'emploi devront s'adresser à « l'Espace Jeune Diplômé » de Lille en indiquant le numéro d'inscription du demandeur d'emploi à l'ANPE. En effet, en l'état, les

seules informations relatives au demandeur d'emploi figurant sur le serveur sont : son numéro d'inscription à l'ANPE, son domaine d'activité, sa zone de mobilité, sa compétence et son profil.

Toutefois, l'ANPE n'exclut pas à terme de mettre en ligne davantage d'informations sur les demandeurs d'emploi, dans le souci de stimuler et d'accélérer les contacts ; il pourrait s'agir notamment des nom et prénoms, de la date de naissance et éventuellement d'une photographie. Les risques d'une utilisation détournée de ces informations sont cependant importants. C'est la raison pour laquelle, en l'état, l'identité des candidats n'est pas accessible directement par le réseau.

Au plan de la protection des données personnelles, il est prévu que les candidats donnent leur accord écrit avant diffusion de leur CV sur le réseau, grâce à une fiche d'autorisation comportant les mentions de l'article 27 de la loi du 6 janvier 1978 et précisant la possibilité pour le demandeur d'emploi de solliciter à tout moment le retrait de son CV du serveur. Par ailleurs, les écrans de consultation doivent préciser la finalité du traitement et donner accès au texte de la loi du 6 janvier 1978 et des sanctions pénales applicables en cas de non-respect de certaines de ses dispositions. Dans tous les cas, le CV est automatiquement retiré à échéance de deux mois, sauf demande expresse de prolongation. Enfin, il est rappelé que les informations sont réservées à un usage strictement privé et que tout usage collectif ou commercial et toute capture d'informations pour enrichir des bases de données commerciales ou publicitaires sont interdits.

Délibération n° 97-073 du 23 septembre 1997 portant avis sur un traitement automatise d'informations nominatives présenté par l'ANPE et dénommé « WWW.ANPE.FR » ayant pour finalité une expérimentation relative à l'amélioration du rapprochement des offres et des demandes d'emplois des jeunes diplômés de la région Nord-Pas-de-Calais

(Demande d'avis n° 533 772)

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 code du travail et notamment ses articles L. 311 -7 et R. 311 -4-1 et suivants ;

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

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

Considérant que l'ANPE a déposé une demande d'avis concernant la mise en service d'un serveur Internet « WWW. ANPE. FR » ayant pour finalité l'amélioration du rapprochement des offres et des demandes d'emplois ;

Considérant que le serveur regroupe une présentation générale de l'ANPE, une information générale des entreprises et des demandeurs d'emplois ainsi qu'un second service mis en œuvre à titre expérimental, en collaboration avec le conseil régional Nord-Pas-de-Calais, la délégation régionale de l'ANPE et l'Union européenne, diffusant les curriculum vitae des demandeurs d'emplois jeunes diplômés et des offres d'emplois à destination des techniciens agents de maîtrise et cadres ;

Considérant que les offres d'emplois en provenance de Sage 2 seront déposées quotidiennement sur le site ; que les curriculum vitae des jeunes diplômés seront déposés une fois par semaine ;

Considérant que des écrans de consultation préciseront la finalité du traitement, et feront référence aux dispositions légales applicables, qu'il s'agisse de la loi du 6 janvier 1978 ou des sanctions pénales qui répriment les infractions à la loi du 6 janvier 1978 ; que sera précisé que les informations sont réservées à un usage strictement privé et que tout usage collectif ou commercial et toute capture d'informations pour enrichir des bases de données commerciales ou publicitaires sont interdits ; Considérant que les informations concernant les demandeurs d'emploi sont le numéro d'inscription à l'ANPE, le domaine d'activité, la zone de mobilité définie en grandes régions, la compétence définie par des mots clés, une zone libre complétée en concertation avec l'agence comportant les commentaires du demandeur d'emploi pour définir au mieux son profil professionnel et le curriculum vitae anonymisé ;

Considérant que chaque offre d'emploi précisera le numéro de l'offre, son intitulé, sa date de création, le secteur d'activité, le lieu de travail, le nombre de postes et leur description, et l'expérience requise ainsi que les coordonnées de la personne à contacter dans l'entreprise en cas d'offre nominative ; Considérant que les demandeurs d'emploi compléteront une fiche d'autorisation comportant les mentions de l'article 27 de la loi du 6 janvier, les données devant être publiées, et la possibilité pour le demandeur d'emploi de demander à tout moment le retrait de son CV du serveur ; que cette fiche d'autorisation précise que le CV sera retiré du serveur au bout de deux mois, sauf demande de prolongation expresse du demandeur ;

Considérant que les sécurités mises en œuvre sont satisfaisantes ;

Émet un avis favorable au projet de décision présenté par l'ANPE.

III. ANNUAIRES SANS FRONTIERES

A. La recommandation du 8 juillet 1997

Depuis le fameux « 22 à Asnières », les possibilités de joindre une personne au téléphone se sont sensiblement perfectionnées ; tandis que l'utilisation du téléphone se généralisait, la liste des abonnés est devenue une fabuleuse source d'informations, la faculté de toucher un nombre important de foyers devenant en soi un enjeu commercial.

Dès 1983, la Commission avait accepté le principe de la cession commerciale des listes d'abonnés au téléphone moyennant des garanties,

notamment sur les tris réalisés, et la possibilité offerte à chacun de s'opposer gratuitement à l'exploitation commerciale de ses données tout en continuant à figurer dans l'annuaire (cf. 4e rapport, p. 89, 6e rapport, p. 68). Ainsi est née la liste orange dont la consécration est intervenue par sa codification en 1992 *(cf.* 13e rapport, p. 223, à propos de l'article R. 10-1 du code des postes et télécommunications).

Plus récemment, l'internationalisation et l'essor des télécommunications ont conféré aux annuaires une valeur croissante. De fait, à la veille de son bicentenaire, l'annuaire du téléphone devient la pièce maîtresse de la société de l'information et n'en finit pas de se décliner en des supports et des utilisations multiples.

Dès que la possibilité technique de diffuser des données de l'annuaire sur Internet ou sur CD ROM a été acquise, la CNIL a fait observer que des garanties spécifiques devaient être offertes aux personnes. La CNIL a ainsi demandé que toute personne puisse, en s'adressant à l'opérateur auprès duquel elle est abonnée, ou à son distributeur, s'opposer gratuitement à ce que les informations nominatives la concernant soient mentionnées dans un annuaire distribué ou diffusé sur support électronique. Cette position de la CNIL est conforme à celle prise par d'autres autorités de protection des données en Europe ou par des juridictions étrangères (cf. 17e rapport, p. 72 et sur la notion de protection adéquate, voir *infra,* 2e partie, chapitre 2).

Cependant, dans le souci de donner une solennité particulière à sa doctrine en la matière, la CNIL a adopté une recommandation de portée générale sur les annuaires. En effet, à la perspective de diffusion de l'annuaire sur Internet, s'ajoutaient l'apparition de procédés de recherche de l'identité des personnes à partir du simple numéro de téléphone (annuaire inversé). Par ailleurs, la CNIL, instruite par l'expérience du télédéchargement de l'annuaire électronique diffusé sur le minitel *(cf.* 13e rapport, p. 221, 15e rapport, p. 91, 16e rapport, p. 128 et 17e rapport, p. 35), a imaginé des solutions propres à éviter que la volonté des personnes s'opposant à l'utilisation commerciale de leurs données ne soit détournée ou méconnue. Enfin, la CNIL était consciente que ces bouleversements se déroulaient, d'une part dans un contexte de forte concurrence entre les éditeurs de listes d'abonnés et, d'autre part, en l'absence de publication du décret relatif à l'annuaire universel prévu par l'article L. 35-4 du code des postes et télécommunications, modifié par la loi de réglementation des télécommunications n° 96-659, du 26 juillet 1996 *(cf. infra* 3e partie, chapitre 11).

C'est dans cet esprit que la Commission a recommandé, par délibération n° 97-060 du 8 juillet 1997, que :

- tout abonné soit clairement et préalablement informé que son numéro de téléphone peut figurer dans un annuaire inversé accessible à tout public afin de pouvoir s'opposer, hors les cas justifiés par la sauvegarde de la vie humaine ou la sécurité publique, à la communication de ses nom et adresse à partir de son numéro de téléphone ;
- que tout abonné soit préalablement informé par les éditeurs d'annuaires sur Internet d'une diffusion des données le concernant sur un tel réseau et soit mis en mesure de s'opposer à une telle diffusion ;

- que l'exercice de ces droits d'opposition soit gratuit et que des moyens fiables et aisés à mettre en œuvre soient mis à la disposition des abonnés souhaitant exercer ces droits ;
- que les éditeurs d'annuaires, quel que soit le support d'édition d'un annuaires (papier, CD-rom...), permettent à tout utilisateur de repérer immédiatement ceux des abonnés qui auront souhaité interdire ou limiter l'utilisation, notamment commerciale, des données nominatives les concernant.

Par ailleurs, la Commission a rappelé :
- que ces services d'annuaire inversé et de recherche inversée doivent, comme les traitements relatifs à la constitution d'annuaires téléphoniques, être déclarés auprès de la CNIL ;
- que la diffusion d'annuaires téléphoniques sur les réseaux internationaux ouverts tel Internet doit elle aussi être soumise à l'avis de la CNIL.

C'est dans le souci de protéger de façon très pragmatique les droits des personnes que la Commission a demandé que l'exercice du droit d'opposition demeure gratuit et facile à mettre en œuvre pour les abonnés. Mais, la CNIL est allée plus loin en incitant les éditeurs d'annuaires, quelqu'en soit le support, à permettre le repérage immédiat des abonnés qui souhaitent interdire ou limiter l'utilisation, notamment commerciale, des données nominatives les concernant.

Délibération n° 97-060 du 8 juillet 1997 portant recommandation relative aux annuaires en matière de télécommunications

La Commission nationale de l'informatique et des libertés,

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

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

Vu le code des postes et télécommunications, ensemble la loi n° 96-659 du 26 juillet 1996 de réglementation de télécommunications et le décret n° 96-1175 du 27 décembre 1996 relatif aux clauses types des cahiers des charges associés aux autorisations attribuées en application des articles L. 33-1 et L. 34-1 du code des postes et télécommunications ;

Considérant que la publication de listes d'abonnés ou d'utilisateurs des réseaux ou services de télécommunications est libre, sous réserve de la protection des droits des personnes concernées ; que les traitements mis en œuvre aux fins d'établissement de ces listes constituent des traitements automatisés d'informations nominatives au sens de la loi du 6 janvier 1978 ; qu'en conséquence, les dispositions protectrices de la liberté individuelle et de la vie privée prévues par cette loi sont applicables aux listes d'abonnés qui, quelque soit le support sur lequel elles sont éditées (support papier, ou support électronique), sont communément appelées annuaires ;

Considérant que les garanties reconnues à ce jour aux abonnés et aux utilisateurs des réseaux ou services de télécommunications, consistent principalement à offrir la possibilité, d'une part, de s'opposer à ce que les informations nominatives les concernant soient mentionnées dans les listes d'abonnés (liste rouge), d'autre part, d'interdire que ces informations soient utilisées dans des opérations commerciales (listes orange et safran) ; qu'en outre, la loi du 26 juillet 1996 de réglementation des télécommunications a reconnu aux abonnés le droit de demander, sous certaines conditions, l'inscription incomplète de leur adresse ainsi que l'inscription de la seule initiale de leur prénom dans les listes d'abonnés diffusées ; Considérant que l'évolution des techniques informatiques et les nouvelles technologies de l'information permettent désormais, d'une part, de rechercher le nom et l'adresse d'un abonné, à partir d'un numéro de téléphone, d'autre part, de rendre accessible par toute personne, quelque soit son lieu de résidence dans le monde, via un réseau international ouvert tel Internet, les données nominatives mentionnées dans un annuaire ; que ces nouveaux traitements doivent être appréciés au regard de leurs éventuelles conséquences sur la vie privée des personnes ;

Sur les annuaires inversés et les services de recherche inversée

Considérant qu'un annuaire inversé permet d'obtenir les nom et adresse d'un abonné, à partir d'un numéro de téléphone ; que le consentement d'un abonné à figurer dans un annuaire téléphonique ne préjuge pas de son consentement à ce qu'une personne puisse rechercher ses noms et adresse, alors même qu'elle n'aurait connaissance que d'un numéro de téléphone, voire d'une partie d'un numéro de téléphone ;

Considérant, en outre, que la combinaison d'un annuaire inversé avec une facture détaillée ou un autocommutateur téléphonique qui enregistre les numéros de téléphone des abonnés appelés, conduit à divulguer au titulaire de la facture, l'identité et l'adresse de tous les abonnés appelés ; Considérant que si le recours à un annuaire inversé peut servir des intérêts légitimes, tels que la sauvegarde de la vie humaine ou la sécurité publique, la divulgation du nom et de l'adresse d'un abonné à partir de la seule connaissance d'un numéro de téléphone est de nature à constituer, si elle est opérée à l'égard de personnes n'ayant pas préalablement été mises en mesure de s'opposer par un moyen facile et fiable à ce qu'un tel dispositif soit utilisé à leur égara, une collecte déloyale d'informations nominatives au sens de l'article 25 de la loi du 6 janvier 1978 ;

Sur la diffusion d'annuaires sur un réseau international ouvert

Considérant que la diffusion de données nominatives sur un réseau international ouvert, tel Internet, comporte des risques inhérents à la structure de ce réseau, tels que leur captation, leur falsification et le détournement de leur finalité ; qu'on ne peut, en raison de ces risques, présumer qu'un abonné figurant dans un annuaire édité en France, consente à ce que les données nominatives le concernant, même s'il en a limité l'inscription ou l'utilisation, soient diffusées au niveau international ;

Considérant en particulier que la possibilité technique pour tout utilisateur d'Internet de télédécharger les données diffusées sur le réseau, accroît les risques de détournement de finalité du traitement de ces informations ;

qu'ainsi, la protection particulière garantie par la loi française aux abonnés qui s'opposent à toute utilisation commerciale des données les concernant, pourrait perdre tout effet, surtout lorsque l'accès à ces informations s'opérera depuis le territoire d'un État n'assurant pas aux données personnelles une protection adéquate ;

Considérant qu'il résulte, tant de la Convention 108 du 28 janvier 1981 du Conseil de l'Europe que de la directive adoptée le 25 octobre 1995 par le Conseil et le Parlement européen sur la protection des données personnelles et la libre circulation de ces données que les flux transfrontières de données ne peuvent, en principe, avoir lieu qu'en direction d'un État assurant un niveau de protection adéquat ;

Considérant que la CNIL recommande, de manière générale, que lorsque des données nominatives sont diffusées sur Internet, les personnes concernées soient clairement informées des risques inhérents à la nature de ce réseau et de leur droit de s'opposer à une telle diffusion, préalablement à celle-ci et ultérieurement à tout moment ; que cette recommandation s'impose avec d'autant plus de force que les abonnés au téléphone ne sont pas tous utilisateurs d'un réseau international ouvert tel Internet ;

Sur la garantie effective du respect des droits des personnes

Considérant que les éditeurs de listes d'abonnés doivent assurer l'application effective de ces droits par la mise en œuvre de procédés permettant à tout utilisateur de ces listes le repérage immédiat des abonnés ayant interdit l'utilisation commerciale des données nominatives les concernant, celui des abonnés s'étant opposés à ce que les informations nominatives les concernant soient diffusées sur un réseau international ouvert, ainsi que celui des abonnés s'étant opposés au traitement des données nominatives les concernant par un service de recherche inversée ou d'annuaire inversé ;

Considérant que la présente recommandation vise à assurer aux personnes concernées des droits et des garanties identiques, quelque soit le fournisseur de ces services ;

Rappelle :
— que les services d'annuaire inversé et de recherche inversée constituent des traitements automatisés d'informations nominatives au sens de l'article 5 de la loi du 6 janvier 1978 ; que ces traitements doivent faire l'objet de demandes d'avis ou de déclarations ordinaires spécifiques ;
— que la diffusion sur un réseau international ouvert tel Internet de listes d'abonnés ou d'utilisateurs des réseaux ou services de télécommunications, doit être soumise à la CNIL en application des articles 24 de la loi du 6 janvier 1978 et 12 de la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe.

Recommande :
- que les abonnés soient clairement et préalablement informés par les éditeurs de services de recherche inversée ou d'annuaires inversés de l'éventualité que leur numéro de téléphone figure dans un service d'annuaire inversé accessible à tout public ;
- que les abonnés puissent s'opposer, hors les cas justifiés par la sauve garde de la vie humaine ou la sécurité publique, préalablement, gratuite ment et sans avoir à indiquer de motif, ainsi qu'ultérieurement à tout moment,

à l'utilisation de leur numéro de téléphone dans un service de recherche inversée ou d'annuaire inversé.

Recommande :

- que les abonnés soient clairement et préalablement informés par les éditeurs d'annuaires sur Internet, des risques inhérents à la diffusion sur un réseau international ouvert des données les concernant ;
- que les abonnés puissent s'opposer gratuitement et sans avoir à indiquer de motif, ainsi qu'ultérieurement à tout moment, à la diffusion sur un réseau international ouvert des données les concernant.

Recommande :

— que les éditeurs de listes d'abonnés assurent l'application effective des droits et des garanties conférés aux abonnés par la mise en oeuvre de procédés permettant à tout utilisateur de ces listes le repérage immédiat des abonnés ayant interdit l'utilisation commerciale des données nominatives les concernant, celui des abonnés s'étant opposés à ce que les informations nominatives les concernant soient diffusées sur un réseau international ouvert, ainsi que celui des abonnés s'étant opposés au traitement des données nominatives les concernant par un service de recherche inversée ou d'annuaire inversé.

B. Une recommandation suivie d'effets

La recommandation n° 97-60 du 8 juillet 1997 relative aux annuaires en matière de télécommunications, qui a été généralement saluée par la presse et les spécialistes, a rapidement été suivie d'effets.

Ainsi, à l'occasion du basculement de son annuaire sur Internet qui est intervenu au début de l'année 1998, France Télécom a respecté les deux droits d'opposition prescrits par la CNIL dans sa recommandation, c'est-à-dire le droit d'opposition à la diffusion de ses données, sur Internet comme sur tout autre support, gratuitement et sans avoir à en donner le motif, et le droit d'opposition à figurer dans un annuaire inversé. De même, France Télécom s'est engagé à ce que l'information annuelle donnée aux abonnés à propos de la liste orange couvre désormais l'ensemble de leurs droits.

Par ailleurs, une société, qui diffuse sur minitel un service de recherche inversée et qui a souhaité basculer sur Internet l'annuaire des abonnés de France Télécom, a diffusé un courrier à l'ensemble des abonnés figurant dans l'annuaire (métropole et DOM-TOM), afin de les informer des caractéristiques du service de recherche inversée et de leur possibilité de s'inscrire gratuitement sur une ou plusieurs listes d'opposition. Trois types de liste étaient en l'espèce proposés : une liste (« Net ») regroupant les personnes ne souhaitant pas figurer dans un annuaire diffusé sur Internet et sur CD-ROM, une liste (« verte ») regroupant les personnes ne désirant pas apparaître dans un service d'annuaire inversé ou faire l'objet d'une recherche inversée, une liste (« blanche ») regroupant les personnes qui s'opposent à l'utilisation de leurs données à des fins de prospection commerciale par téléphone.

Par ailleurs, *cette* société s'est engagée, d'une part à procéder chaque année à la distribution de ce courrier aux 23 millions de foyers français et d'autre part, à faire bénéficier de ses listes, à un faible coût, toute entreprise qui fournit des services d'annuaire inversé ou qui souhaite diffuser sur Internet un annuaire téléphonique, ou encore toute société qui veut régulariser ses fichiers en supprimant les personnes qui se sont opposées à faire l'objet de prospections commerciales.

IV. CYBERCONSOMMATEURS ET CYBERPROSPECTS

A. Un marché mondial à domicile : le commerce électronique

Le commerce électronique n'est certes pas né avec l'Internet, mais l'utilisation de ce réseau en bouleverse radicalement les perspectives. D'abord limité au monde des entreprises et des administrations, le voici qui s'ouvre aux petites entreprises. À terme, le développement des réseaux de télécommunication, dont l'Internet est une illustration, devrait occuper une place importante dans une offre mondiale de produits et services, et constituer un maillage informationnel sans précédent pour des commerçants en quête de nouveaux clients. Encore balbutiant, l'Internet commercial devrait rapidement constituer en France, comme déjà au États-Unis, un véritable support de vente et, d'ailleurs, de nombreuses sociétés commerciales françaises estiment déjà indispensable d'être présentes sur le « web ».

L'Internet commercial se révèle en effet bien tentant : coût relativement bas des opérations, abolition des distances, faculté d'atteindre des dizaines de millions de personnes et surtout possibilité de mettre en contact des commerçants et des consommateurs du monde entier par le biais de sites ouverts 24h/24. En outre, l'exploitation des traces des connexions que permet la technologie d'Internet offre la possibilité d'établir des profils d'achats ou de consommation extrêmement ciblés des internautes. De ce point de vue, Internet constitue un vecteur de vente ou de prospection jamais égalé : c'est un peu, à l'échelle du monde, la mémoire d'une boulangère, qui n'ignore rien de sa clientèle. Le village global, slogan de la société de l'information, c'est d'abord une galerie commerciale à l'échelle de la planète.

Conscients de l'enjeu porté par le commerce électronique dans le domaine de la protection des données, les pouvoirs publics ont eu le souci d'associer la CNIL à leurs réflexions à ce sujet. C'est ainsi que le Gouvernement a saisi la CNIL en 1997, afin de recueillir sa position avant de déterminer les actions à mener ou les principes à défendre en ce qui concerne la protection des personnes dans le cadre du commerce électronique. Cette consultation faisait suite à la publication par la Commission européenne d'une communication intitulée *Une initiative européenne sur le commerce électronique* et consti-

tuait un prélude au grand débat public qui devait s'ouvrir à la lumière du rapport «Lorentz» sur les enjeux du commerce électronique, remis au ministre de l'Économie et des Finances en janvier 1998.

Dans le cadre de sa mission, la CNIL avait déjà pu mesurer la nécessité impérieuse de protéger les données personnelles sur les réseaux, dont Internet, s'agissant en particulier du commerce électronique. En effet, les déclarations de traitement de données adressées à la CNIL, rendent parfaitement compte de la quantité et de la nature des données personnelles qui sont brassées eu égard à la diversité des biens et services disponibles sur le net (agences matrimoniales, services boursiers, agences de voyage, services d'assurance, galeries commerciales...).

La connaissance de ce marché repose sur l'étude du taux de fréquentation des sites commerçants et l'analyse du comportement des utilisateurs qui se connectent ; la force commerciale du réseau réside en effet pour une bonne part dans les informations personnelles qui permettent de mieux connaître le prospect, le client et le marché en général, dans ses aspects les plus fins, notamment en matière publicitaire.

Or, la spécificité de l'Internet au regard de la protection des données est précisément de pouvoir drainer une somme considérable d'informations. En effet, au-delà des renseignements qui peuvent être recueillis par l'envoi de courriers électroniques ou l'exploitation des formulaires remplis par l'utilisateur en ligne ou encore la participation à des forums de discussion, souvent assortis de propositions de recevoir des documents de prospection par « e-mail », Internet offre un potentiel technique de « traçage » comportemental des internautes, dont les fameux *cookies* [1] constituent l'exemple le plus spectaculaire. Pour les marchands sur l'Internet, il s'agit de personnaliser l'offre d'information en ciblant au plus près le consommateur afin que chaque internaute puisse à terme disposer d'une information quasiment sur mesure (marketing *« one to one »).* Au regard de la protection des données, si l'exploitation à des fins commerciales des traces de consultation ou des informations communiquées par les utilisateurs constitue une opportunité sans précédent pour les entreprises commerciales, il convient que les principes généraux des législations de protection des données — information, transparence, droit d'opposition pour tous — continuent à s'appliquer dans ce domaine comme dans d'autres.

Ainsi, au fil de ses expertises, la CNIL a-t-elle dégagé des principes élémentaires en matière de protection des personnes au regard du commerce électronique sur Internet, principes qui ne sont autres que ceux qu'elle avait, depuis longtemps, dégagés quant à l'utilisation d'autres supports.

S'agissant de la collecte et de l'exploitation des mél (ou « e-mail ») à des fins commerciales, la CNIL estime indispensable de garantir à tout internaute quelques droits essentiels :

[1] Un *cookies* est un fichier constitué par un serveur et enregistré sur le disque dur de l'ordinateur de l'internaute.

- le droit de consulter un site marchand sans avoir à s'identifier par ses nom, prénom ou mél ;
- le droit de s'opposer à recevoir, par mél, des documents de prospection commerciale non sollicitées ;
- le droit de refuser que son mél puisse être cédé à un tiers ou utilisé pour le compte d'un tiers sans son contentement.

En ce qui concerne l'établissement de profils de consommation à partir des historiques de transactions et du comportement de l'utilisateur, la CNIL considère qu'il convient de limiter le nombre des renseignements personnels demandés en ligne à ce qu'exige la finalité du traitement, et soutient les initiatives qui peuvent concourir à protéger, dans le respect évidemment de l'ordre public, un certain anonymat sur Internet.

Enfin, s'agissant du potentiel technique de l'Internet à créer des traitements invisibles de données personnelles, la CNIL estime qu'il faut au minimum procéder à une large information des utilisateurs d'Internet.

L'existence de ces traitements invisibles de données personnelles, constitués le plus souvent à l'insu des personnes, impose naturellement de conduire une réflexion approfondie sur le traitement loyal des données, la sécurité et le droit d'accès des intéressés. Tel est notamment l'objet des travaux menés par le groupe européen sur les réseaux internationaux (GERI), créé en 1995, à l'initiative de la CNIL, lors de la conférence européenne des commissaires à la protection des données. Cependant, la Commission estime d'ores et déjà que tous les sites commerciaux devraient indiquer clairement aux personnes concernées, notamment en application de l'article 10 de la directive européenne du 24 octobre 1995, l'utilisation qui sera faite de leurs données, le recours éventuel à des *cookies,* les destinataires des données, l'éventuelle cession à des tiers des informations et, le cas échéant, la possibilité de s'y opposer par le moyen le plus simple qui consiste à apposer une case à cocher par les internautes ne souhaitant pas voir leurs données cédées.

B. Publicité dynamique et marketing interactif

La publicité s'accroît de jour en jour sur le net et commence à devenir une source importante de revenus pour les prestataires de services Internet. En effet, des sociétés, notamment celles qui mettent en œuvre des moteurs de recherche par mots-clés ou thématiques (Yahoo, Altavista...), sont en général rémunérées par les annonceurs pour afficher directement, dans une fenêtre supplémentaire de l'écran, des messages publicitaires. Ainsi, l'exploitation des données comportementales recueillies sur l'internaute permet-elle d'adapter, dans l'instant, la publicité utile au profil de celui-ci. Le temps n'est plus à l'argumentaire de vente à l'attention du plus grand nombre, mais au ciblage savant de la future clientèle : les cyberconsommateurs ne sont plus également prospectés, ils deviennent personnellement prospectés.

De même, des fournisseurs d'accès acceptent désormais de fournir gratuitement des adresses électroniques à condition que les internautes acceptent leur utilisation à des fins de prospection adaptée. Ainsi, la CNIL a été saisie d'une demande de conseil, par la société « Multiversions France », à propos d'un dispositif original de fourniture d'accès et de services sur Internet, baptisé « None Networks ».

En contrepartie de l'autorisation d'utiliser les données comportementales des abonnés, ces derniers se voient offrir la gratuité de l'accès, une remise de 30 % sur le coût des communications et la mise à disposition de deux logiciels spécifiques de navigation, « My Way » et « WebComposite ». Ces logiciels sont conçus pour faciliter la navigation sur Internet dès lors que les centres d'intérêt des utilisateurs sont connus. Dans le cas de « My Way », les centres d'intérêts sont indiqués par l'internaute lors de l'installation du logiciel dans son ordinateur, et le logiciel lui fournit la liste des sites correspondant à ses centres d'intérêts, constamment mise à jour lors de ses connexions ultérieures. Dans le cas de « WebComposite », le logiciel assure automatiquement le suivi comportemental de l'abonné, puis à l'occasion de toute nouvelle recherche, crée un lien avec des sites connexes ou ajoute un espace publicitaire.

Ainsi, les clients de « None Networks » doivent-ils accepter, pour bénéficier des offres, l'utilisation de leurs données comportementales sous forme de statistiques anonymes et, sous réserve d'une autorisation expresse, sous forme nominative. Toutefois, plusieurs garanties de protection des données leur sont offertes. Ainsi, il est prévu qu'aucun profil comportemental ne puisse être réalisé à partir des consultations de sites en rapport avec les mœurs et le domaine religieux, politique ou syndical, champs qui relèvent des données sensibles énumérées par l'article 31 de la loi du 6 janvier 1978. De plus, l'internaute peut s'opposer à tout moment, de manière permanente ou ponctuelle, dans la limite de trois thèmes, à l'enregistrement des sites qu'il souhaite consulter et ce, sans avoir à invoquer de raisons légitimes ; de même, la possibilité lui est offerte de s'opposer ponctuellement à la mise en mémoire des références d'un site qu'il vient de visiter.

Enfin, la Commission a pris acte de ce que chaque abonné est informé, par le contrat et par le serveur, de l'utilisation des données collectées et de la finalité du traitement, ainsi que de son droit de ne pas autoriser la cession à des tiers des données comportementales nominatives le concernant, étant observé que son accord à une telle cession devra être exprès et que le défaut d'un tel accord n'aura pas d'incidence sur l'exécution du contrat.

Toutefois ce type de solutions, qui repose sur le choix individuel de la personne, présente incontestablement des limites. En effet, il n'a pas échappé à la Commission que le fait de lier l'accès au réseau à la fourniture d'informations non nécessaires à la réalisation de cette prestation conduit à faire dépendre la protection de la vie privée des revenus des utilisateurs. En définitive, la CNIL s'inquiète de ce qu'un simple contrat puisse conduire l'internaute à l'abandon de certains de ses droits garantis par la loi du 6 janvier 1978 et la directive 95/46/CE du 24 octobre 1995.

Chapitre 2

LES FLUX TRANSFRONTIÈRES À L'ÉPREUVE DES RÉSEAUX

La protection des données ne cesse de progresser dans le monde. Désormais, tous les pays de l'Union européenne sont dotés d'une législation générale dans ce domaine. Dix-neuf pays ont en outre signé et ratifié la Convention 108 du Conseil de l'Europe, dont récemment l'Italie, la Grèce et la Suisse : ce sont là des progrès encourageants.

Pourtant, depuis vingt-cinq ans, date d'adoption de la première loi de protection par la Suède, tout a changé ou presque : d'abord, la nature des données traitées dans les fichiers informatiques s'est diversifiée à l'infini, puisqu'il peut s'agir désormais d'informations relatives au comportement, aux habitudes, aux trajets, à l'image, à la voix ou encore des données génétiques. La quantité des informations personnelles recensées et exploitées dans des bases de données s'est accrue au fur et à mesure que la puissance des techniques informatiques permettait un traitement rapide de forts volumes d'informations. Le déploiement d'infrastructures mondiales d'échanges de données, dont l'Internet constitue le meilleur exemple, a accentué ces phénomènes. Enfin, et ce n'est pas le plus neutre des constats, les grandes banques de données, en tout cas les plus complètes, sont désormais d'origine privée.

Aussi, la question de la protection des données personnelles dépasse-t-elle le seul rapport Gouvernement-citoyens et concerne-t-elle tout autant les relations particuliers-entreprises ou encore consommateurs-commerçants. Le développement intensif du marketing direct personnalisé *(« one to one »),* la recherche d'informations par les entreprises, notamment pour apprécier le risque économique des personnes, enfin, le décloisonnement des secteurs d'activité, à l'exemple des banques qui font de l'assurance ou des compagnies aériennes qui se lancent dans des services hôteliers, ont multiplié les flux transfrontières de données.

Toutes les législations nationales de protection des données se sont préoccupées du problème posé par les transmissions d'informations nominatives vers les Etats ne disposant pas d'une loi dans ce domaine. La loi du 6 janvier 1978 comme la Convention du Conseil de l'Europe du 28 janvier 1981 subordonnent les flux transfrontières de données à la condition que l'État ou l'organisme destinataire offre une protection équivalente à celle qui est garantie par nos législations.

La CNIL a imaginé, dès la fin des années 1980, un dispositif original qui permet d'assurer cette garantie : la conclusion d'un contrat de protection des données entre l'organisme expéditeur et l'organisme destinataire. Cette doctrine a été élaborée à l'occasion de l'examen d'un flux transfrontière entre la société FIAT-France et sa maison mère située en Italie, pays alors dépourvu de loi de protection des données. Au plan européen et international, la position de la CNIL a rencontré un large écho et a fait jurisprudence.

La directive européenne du 24 octobre 1995 relative à la protection des données personnelles et à la libre circulation de ces données s'est inspirée de ce principe général : les droits des personnes à l'égard du traitement informatique de leurs données doivent suivre ces données, lorsque ces informations traversent les frontières. Les flux transfrontières, auxquels Internet donne une ampleur nouvelle, doivent ainsi contribuer à propager dans le monde la culture européenne de protection des données.

I. LA NOTION DE PROTECTION ADEQUATE

L'article 25 de la directive européenne fait obligation aux Etats de prévoir que « le transfert vers un pays tiers de données à caractère personnel [...] ne peut avoir lieu que si [...] le pays tiers assure un niveau de protection adéquat ». Cette protection adéquate doit s'apprécier au regard de celle qui est offerte en Europe, selon les termes même de la directive. Si ce terme « adéquat » peut paraître en retrait sur l'exigence d'un niveau de protection « équivalent », formulée précisément par la loi du 6 janvier 1978 et la Convention 108 du Conseil de l'Europe, il demeure que le principe énoncé dans la directive européenne est essentiel.

La directive donne quelques indications sur la méthode qui doit être suivie pour apprécier si le niveau de protection des données est adéquat ou non : « Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transfert de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée des traitements envisagés, les pays d'origine et de destination finale, les règles de droit générales ou sectorielles en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

Cette méthode est familière à la CNIL qui a eu l'occasion dès 1989 de préciser les vérifications auxquelles elle procédait pour apprécier si un État étranger offrait ou non un niveau de protection équivalente, au sens de l'article 12 de la Convention 108 du Conseil de l'Europe (cf. 10e rapport, p. 45 et suivantes)

La Commission n'a cependant jamais procédé à une analyse *in abstracto* du degré de protection offert par un pays tiers.

Ainsi, en 1984, la CNIL avait été saisie d'une demande d'avis relative à la transmission sur support magnétique par le Gouvernement français au Gouvernement de Côte-d'Ivoire d'informations nominatives sur les agents français mis à la disposition de ce pays, dans le cadre de la coopération technique. Elle a, en l'espèce, considéré que les informations enregistrées dans le traitement étaient d'ordre purement administratif, qu'il s'agissait essentiellement d'assurer la paie de ces agents, que les coopérants français étaient informés de ce transfert et pouvaient exercer leur droit d'accès. Ces conditions l'ont conduite à émettre un avis favorable à ce transfert sans exiger de garanties supplémentaires.

Si cette méthode d'appréciation au cas par cas, est utile, il convient toutefois d'éviter que les États européens puissent porter des appréciations divergentes sur la protection offerte, dans tel secteur d'activité, par tel pays tiers. C'est la raison pour laquelle la directive européenne a prévu des mécanismes d'information réciproque entre autorités nationales de protection des données. Ainsi, l'article 25-3 fait obligation aux États-membres et à la Commission de s'informer mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat. En cas de divergence d'appréciation entre États européens, la Commission européenne peut constater soit que le pays tiers en cause n'assure pas un niveau de protection adéquat (dans ce cas, les États-membres doivent prendre toutes les mesures nécessaires en vue d'empêcher un transfert de données de même nature vers le pays tiers en cause), soit que le pays tiers assure un niveau de protection adéquat au sens de la directive (dans ce cas, les États-membres doivent également se conformer à la décision de la Commission).

La Commission européenne est donc appelée à jouer un rôle tout à fait déterminant dans l'appréciation du niveau de protection offert par les pays tiers. L'article 25 de la directive européenne lui reconnaît d'ailleurs le pouvoir d'engager « au moment opportun » des négociations internationales avec les pays n'assurant pas un niveau de protection adéquat.

Cependant la Commission européenne n'agit pas seule. En cas de divergence d'appréciation entre États-membres, la Commission doit recueillir l'avis d'un comité, prévu par l'article 31 de la directive, qui est composé de représentants des États-membres. Lorsque la Commission européenne souhaite arrêter des mesures qui ne seraient pas conformes à l'avis de ce comité, c'est au Conseil des ministres de trancher.

Il convient également de signaler le rôle extrêmement important qui est confié à un groupe composé de représentants de chacune des autorités natio-

nales de contrôle de chacun des pays membres. Ce groupe, institué par l'article 29 de la directive, s'est d'ailleurs réuni à plusieurs reprises depuis la publication du texte européen et sans attendre que la directive soit transposée dans chacun des États-membres. Ce « groupe de protection des personnes à l'égard du traitement des données à caractère personnel » a pour mission générale de contribuer à une mise en œuvre homogène des dispositions nationales prises en application de la directive et de donner à la Commission européenne un avis sur le niveau de protection dans les pays tiers.

Il consacre la pratique ancienne des autorités européennes de protection des données de se réunir, deux fois par an, pour débattre ensemble des problèmes communs de protection des données, comme chacun des précédents rapports d'activité de la CNIL en témoigne, tant il est vrai que la problématique des flux transfrontières n'est pas nouvelle.

Il doit être souligné enfin que la directive ménage certaines dérogations destinées à permettre des transferts de données à destination de pays tiers n'assurant pas un niveau de protection adéquat, soit en cas de circonstances particulières énumérées à l'article 26-1 de la directive (ainsi lorsque la personne a « indubitablement » donné son consentement au transfert envisagé, lorsque le transfert est nécessaire à l'exécution d'un contrat, ou à la sauvegarde de l'intérêt vital, etc.) ou lorsque le responsable du traitement offre des garanties particulières en matière de protection des données, notamment par la voie de clauses contractuelles appropriées (article 26.2).

Cette dernière disposition consacre la doctrine suivie par la CNIL depuis de nombreuses années et connue au plan européen et international sous l'appellation « doctrine FIAT » *(cf. Les libertés et l'informatique -20 délibérations commentées* — éd. La Documentation française, chapitre 7, p 63). Il s'agit d'étendre à un pays tiers, par un contrat passé entre l'organisme expéditeur des données et l'organisme destinataire, le dispositif de garanties offert en France, la garantie suivant en quelque sorte la donnée transférée.

La directive européenne accorde une importance particulière à ce dispositif de garanties contractuelles. En effet, d'une part, chaque État membre doit informer la Commission et les autres États-membres des autorisations accordées sur le fondement des garanties contractuelles. Chaque État membre peut alors exprimer une opposition à l'autorisation accordée au motif que les garanties contractuelles sont insuffisantes, la Commission devant alors trancher cette divergence de vue dans les conditions de procédures décrites ci-dessus (avis du Comité prévu par l'article 31). D'autre part, la Commission européenne peut décider que certaines clauses contractuelles types offrent des garanties suffisantes pour que les transferts de données puissent être autorisés à destination d'un pays tiers n'offrant pas un niveau de protection adéquat. Dans ce cas, les États membres doivent prendre les mesures nécessaires pour se conformer à la décision de la Commission.

Tel est le dispositif d'avenir en Europe.

Il a déjà incontestablement contribué à une prise de conscience de la part des partenaires commerciaux des pays européens qui ne sont pas dotés d'une loi de protection des données, tant les flux transfrontières sont désormais nombreux, surtout à l'heure d'Internet.

II. LA REGULATION DES FLUX

La CNIL a été saisie par le ministère de l'Economie, des Finances et de l'Industrie d'une demande d'avis concernant un système d'échanges de renseignements douaniers entre les États. En effet, le ministère a souhaité constituer une base de données, dénommée « MARINFO », pour gérer les informations relatives au trafic illicite de stupéfiants par mer, que les Etats signataires de la Convention des Nations unies du 19 décembre 1988 contre le trafic de stupéfiants et de substances psychotropes se sont engagés à transmettre dans le cadre de leur participation à un dispositif coordonné de coopération internationale, tel est l'objet du réseau « MARINFO ».

Ce réseau constitue un outil indispensable aux actions d'investigation, de recherche et de travail de renseignement, outil qui été optimisé grâce à un système d'échanges de données sous forme de télex normalisés, d'abord entre des pays européens du nord (système « MARINFO NORD » : Royaume-Uni, Irlande, Belgique, Pays-Bas...), puis étendu aux Etats riverains de la Méditerranée (« MARINFO SUD » : France, Italie, Espagne...). La France, représentée par la direction nationale du renseignement et des enquêtes douanières (DNRED), et l'Allemagne sont les deux pays coordonnateurs de « MARINFO NORD » et de « MARINFO SUD » ; ils s'échangent à ce titre, sous forme de télex, les informations dont ils disposent, puis les transmettent aux membres de leur réseau respectif.

Dans ce cadre, la base « MARINFO » qui a vocation à être alimentée par les informations figurant sur l'ensemble des télex et télécopies transmis à la DNRED devra, d'une part constituer une aide à la présélection des contrôler à effectuer et, d'autre part, fournir des résultats statistiques sur l'efficacité des échanges, assortis d'indications sur l'évolution des filières et des modes opératoires et permettre ainsi d'enrichir les signalements transmis aux autres États membres.

À cet effet, la base « MARINFO » centralise des informations concernant les conteneurs, les bateaux, les contrôles effectués, les sociétés et les personnes physiques en cause, c'est-à-dire leurs identité, date de naissance et nationalité, ainsi que le motif du signalement. Il a toutefois été précisé que si l'identité de certains membres d'équipage d'un bateau peut être mentionnée dans un avis de fraude, ces signalements ne porteront en aucun cas sur l'ensemble de l'équipage.

Enfin, la CNIL a rappelé les échanges d'informations avec des pays dépourvus d'une législation sur la protection des données doivent faire l'objet de protocoles d'accord prévoyant l'engagement des autorités étrangères concer-

nées de garantir la confidentialité des données, de respecter la finalité douanière et enfin, d'instaurer un dispositif de contrôle comparable au système de droit d'accès indirect aux informations prévu par l'article 39 de la loi du 6 janvier 1978. Dans ces conditions, un avis favorable a été délivré par la CNIL, qui a demandé à être destinataire des protocoles qui pourront le cas échéant être signés avec de tels pays.

Délibération n° 97-064 du 8 juillet 1997 portant avis sur un projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie concernant un système automatisé de gestion du renseignement sur le trafic de stupéfiants par voie maritime

(Demande d'avis n° 475 713)

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 Convention des Nations unies contre le trafic illicite de stupéfiants et de substances psychotropes, adoptée à Vienne le 19 décembre 1988 et publiée par le décret n° 91-271 du 8 mars 1991 ;

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 des douanes ;

Vu le projet d'arrêté présenté par le ministère de l'Économie, des Finances et de l'Industrie ;

Après avoir entendu Monsieur Thierry Cathala, commissaire 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 « MARINFO », qui est créé au sein de la direction générale des douanes et droits indirects (DGDDI) et dont la gestion est confiée à la direction nationale du renseignement et des enquêtes douanières (DNRED) ;

Considérant que cette base de données a pour objet de centraliser l'ensemble des informations transmises dans le cadre du réseau MARINFO SUD, qui consiste en un système d'échanges, sous forme de télex normalisés, d'informations sur le trafic de drogue par mer ; que participent à MARINFO SUD les services douaniers des grands ports des états proches de la Méditerranée : la France, l'Italie, l'Espagne, le Portugal, Gibraltar et la Grèce ; que la France, représentée par la DNRED, a pour mission de centraliser les avis de fraude sur les conteneurs, les bateaux et leurs itinéraires, qui proviennent de l'ensemble des États adhérant à MARINFO SUD, et de les adresser, si nécessaire, aux autres états membres du réseau intéressés ;

Considérant en outre que la France et l'Allemagne, en qualité de coordon-nateurs respectifs des réseaux MARINFO SUD et de MARINFO NORD — qui relie dans les mêmes conditions les ports de l'Europe du Nord — se communiquent mutuellement les informations en leur possession, lorsque cela s'avère utile, afin de les retransmettre aux autres membres de leur réseau ;

Considérant que le traitement « MARINFO » constitue une base de renseignements opérationnels, dont les finalités sont :
— l'aide à la présélection des expéditions maritimes à contrôler, grâce à la diffusion, auprès des services extérieurs et correspondants de la DNRED dans les grands ports français, des avis de fraude sur les navires, les conteneurs, les envois et les sociétés suspectés d'être liés à un trafic maritime de stupéfiants ;
— la mesure, d'une part, de l'efficacité du groupe MARINFO SUD par l'analyse des résultats obtenus, notamment des comptes rendus de saisie de drogue, et d'autre part, de l'évolution des filières et des modes opératoires ;
— l'enrichissement des signalements transmis aux autres États membres, sur la base des renseignements enregistrés dans le traitement.

Considérant que les informations traitées proviennent :
— des services douaniers des ports français ;
— des autres états qui participent à MARINFO SUD ;
— du Zollkriminal Institut allemand, pour ce qui concerne les messages provenant des états membres de MARINFO NORD.

Considérant que les catégories d'informations susceptibles d'être enregistrées sont :
— en ce qui concerne les conteneurs : le pays d'origine, le numéro, les dimensions, la marchandise, les références du propriétaire et de l'exploitant, l'origine de l'information ;
— en ce qui concerne les bateaux : le nom du navire, le pavillon, le port d'attache, la compagnie maritime affréteur, l'origine de l'information, ainsi que, pour chaque voyage faisant l'objet d'un suivi, les références et l'adresse de l'expéditeur et du destinataire, les dates, pays et ports de chargement et de déchargement ;
— en ce qui concerne les constatations effectuées : la nature de la consta tation, la date, le pays, le motif du contrôle, les lieu et date de la saisie ou du contrôle, la provenance et la nature de la marchandise, la nature des cachettes, le nombre de personnes interpellées, la nature et la quantité du produit stupéfiant ;
— en ce qui concerne les sociétés : le nom ou la raison sociale, le numéro Siret ou Siren, l'adresse ;
— en ce qui concerne les personnes physiques : le nom, le prénom usuel, le sexe, la date de naissance, la nationalité, le motif du signalement.

Considérant que les seules personnes physiques concernées sont les individus liés à l'opération frauduleuse qui fait l'objet du message, et qui sont déjà connus des services douaniers ou à l'égard desquels existent des indices réels de fraude ; qu'en conséquence, si l'identité de certains membres de l'équipage des navires surveillés peut être enregistrée, ces signalements ne portent en aucun cas sur l'ensemble de l'équipage d'un bateau ;

Considérant que le délai de conservation est fixé à trois ans ; qu'en outre, une information pourra être affectée d'une date spécifique de péremption dans le seul but de réduire sa durée de conservation ; qu'enfin, les informa-

tions pourront être effacées à tout moment, dès qu'elles seront considérées comme étant périmées ;

Considérant que seuls les services douaniers déconcentrés et les correspondants douaniers de la DNRED doivent disposer de terminaux reliés à l'application :

- les échelons régionaux de la DNRED ;
- les bureaux aéronavals des douanes de Nantes, Rouen, Marseille et des Antilles,
- les services des directions régionales des douanes spécialisés dans le contrôle des conteneurs ;
- le bureau de l'administration centrale de la DGDDI chargé de la lutte contre la fraude.

Considérant que les autorités étrangères, qui ont qualité, en vertu d'une Convention internationale ratifiée et publiée, pour connaître des informations recueillies par la DNRED, et qui participent aux réseaux MARINFO, peuvent également être destinataires des informations traitées par télex ou de télécopie ; qu'il convient que les échanges de données, qui seront mis en place avec des États ne disposant pas d'une législation en matière de protection des personnes à l'égard du traitement des données à caractère personnel, fassent l'objet de protocoles d'accord, par lesquels les autorités étrangères concernées s'engageront à garantir la confidentialité et à respecter la finalité douanière des signalements transmis par MARINFO, ainsi qu'à mettre en place un dispositif de contrôle propre ou reprenant au moins les dispositions de l'article 39 de la loi du 6 janvier 1978 ; Considérant que le droit d'accès aux informations conservées dans le traitement « MARINFO » et aux dossiers papier correspondant est régi par l'article 39 susmentionné et s'exerce par l'intermédiaire de la Commission nationale de l'informatique et des libertés ; que toutefois, l'article 4 du projet d'arrêté devra être modifié afin de remplacer la formule « auprès de la Commission [...] » par les mots « [...] par l'intermédiaire de la Commission **[...] » ;**

Émet un avis favorable sur le projet d'arrêté présenté par le ministère de l'Économie, des Finances et de l'Industrie, sous réserve que :

- L'alinéa suivant soit ajouté à la fin de l'article 3 :

« Les échanges de données mis en place avec des états ne disposant pas d'une législation en matière de protection des personnes à l'égard du traitement des données à caractère personnel feront l'objet de protocoles d'accord par lesquels les autorités étrangères concernées s'engageront à garantir la confidentialité et à respecter Ta finalité douanière des signalements transmis par MARINFO, ainsi qu'à mettre en place un dispositif de contrôle propre ou reprenant au moins les dispositions de l'article 39 de la loi du 6 janvier 1978 ».

- La formule « auprès de la Commission [...] » soit remplacée à l'article 4 par les mots « [...] par l'intermédiaire de la Commission [...] ».

III. LA SECURISATION DES ECHANGES DE DONNÉES ÉCONOMIQUES

Une société dénommée Full Service Trade System (FSTS), établie aux Bermudes, a déclaré à la CNIL une application baptisée *TradeCard* consistant à sécuriser les transactions commerciales internationales électroniques des PME, et le cas échéant d'entrepreneurs individuels. Cette application de commerce électronique au plan mondial, *(business to business)* constitue une illustration intéressante des flux transfrontières de données et de la recherche d'une protection adéquate des données au regard des règles européennes.

FSTS est une filiale de la « World Trade Center », association de centres de commerce international, répartis dans plus de trois cents villes regroupant près de 500 000 membres dans une centaine de pays. En France, il existe une douzaine de centres de commerce international, pour la majorité contrôlés par les chambres de commerce (Paris, Lyon, Bordeaux, Le Havre, Nantes...). Ces centres de commerce doivent faciliter les échanges internationaux impliquant en particulier les PME-PMI françaises qui peuvent rencontrer d'importantes difficultés lors de la conclusion et de l'exécution des contrats internationaux de vente ou d'achat ou en matière de sécurisation des paiements. La « World Trade Center » a spécialement créé la société FSTS pour développer et exploiter le service *TradeCard* qui vise à offrir aux entreprises un outil informatique pour conclure et exécuter de manière sécurisée des transactions commerciales internationales.

En effet, grâce à un réseau mondial privé, le système *TradeCard,* les entreprises pourront tout à la fois échanger et assurer la conservation et la preuve des documents concrétisant les transactions commerciales internationales (commandes, factures, ordre de paiement, certificats d'assurance...), effectuer les formalités afférentes à ces transactions à un coût réduit. À chaque étape de son intervention, FSTS valide formellement les messages qui transitent par son intermédiaire et en garde une copie sur son serveur localisé également aux Bermudes pendant au moins dix ans, aux fins de preuve des transactions commerciales. Cette durée correspond à la durée de conservation comptable des documents fixée par l'article 189 du code du commerce, mais elle peut s'avérer plus longue si une législation de l'État de l'une des parties à la transaction le prévoit.

Le fonctionnement du système exige de connaître les identités des entreprises adhérentes (raison ou dénomination sociale, identifiant électronique, adresse, téléphone et fax) et de l'institution financière gérant le compte de l'utilisateur importateur, ainsi que son numéro de compte, la disponibilité ou non d'une ligne de crédit, des informations diverses concernant les biens et les conditions de la transaction commerciale (articles, quantité, commandes, factures, conditions tarifaires, moyens de paiement, assurance...), les date et heure de la transaction électronique, les clés utilisées pour le chiffrement des signa-

tures, enfin l'identité du contact de l'entreprise utilisatrice de *TradeCard* (nom, prénom), de sorte que FSTS puisse l'informer des différentes mises à jour.

Au plan de la protection des données personnelles, il convient de relever que les informations peuvent être modifiées en ligne à tout moment par l'utilisateur concerné. Par ailleurs, il est prévu que les dispositions de l'article 27 de la loi du 6 janvier 1978 figurent dans le contrat conclu entre un utilisateur et tout distributeur du logiciel *TradeCard* en France et dans le contrat de licence d'utilisation de ce logiciel.

En effet, toute entreprise souhaitant participer au système *TradeCard* doit faire l'acquisition de la licence d'exploitation du logiciel et souscrire à un contrat d'abonnement qui, du fait de l'absence de législation protectrice des données aux Bermudes, comporte l'engagement que FSTS respectera la législation en vigueur en France en matière de protection des données nominatives. De même, le contrat doit mentionner clairement les finalités et les destinataires des informations, ainsi que les mesures prises pour faire assurer le respect de ces dispositions par les employés et sous-traitants de FSTS.

La sécurisation des transactions commerciales électroniques repose sur le chiffrement de la signature électronique, les autres données demeurent en langage clair sur le serveur FSTS. De plus, chaque entreprise dispose d'un code d'identification, d'un mot de passe pour accéder au réseau et des clefs de chiffrement utilisées.

Il convient de souligner que le réseau utilisé n'est pas Internet, mais un réseau privé virtuel accessible, soit par le réseau commuté, soit par une ligne louée, à partir d'un grand réseau de télécommunication mondiale développé par une société spécialisée dans la commercialisation de réseaux virtuels à valeur ajoutée de portée mondiale.

Au total, la CNIL a estimé que les engagements pris par la FSTS étaient satisfaisants, voire exemplaires pour des fournisseurs de services sur d'autres réseaux internationaux fermés proposés par les grands opérateurs de télécommunications. Compte tenu des intérêts en présence, à savoir la protection du secret des affaires autant que la protection des données nominatives, la Commission a considéré que les mesures de sécurités étaient satisfaites, même si l'utilisation d'une carte à mémoire pour authentifier la personne qui accède au système aurait constitué une meilleure solution que celle du recours à un mot de passe.

Ce dossier illustre le fait que la loi française de protection des données est respectée, dès lors que les données sont collectées sur le territoire national, même par des entreprises qui s'établissent à l'étranger. La directive européenne du 24 octobre 1995, a retenu le même dispositif dans son article 4 faisant obligation au responsable d'un traitement qui n'est pas établi sur le territoire de la Communauté, d'appliquer les dispositions nationales de l'État membre au sein duquel il recourt à des moyens de traitement de données. Il est essentiel de comprendre qu'une telle prescription est de nature à éviter la création de « paradis informatiques » où les données pourraient être exploitées en dehors

de tout cadre juridique. Toutefois, la mise en place d'un véritable dispositif de coopération internationale devrait compléter ces garanties afin de permettre la vérification sur place de l'effectivité des mesures prises par une entreprise en faveur de la protection des données.

IV. LE FOISONNEMENT DES INITIATIVES

Avant même son adoption, la directive européenne du 24 octobre 1995 a suscité une prise de conscience nouvelle de la part des États n'étant pas dotés de législation générale en matière de protection des données. C'est ainsi que les partenaires du *G7,* lors de la conférence ministérielle tenue à Bruxelles les 25 et 26 février 1995, se sont engagés à établir des dispositions nationales et régionales en matière de protection des données, à en assurer le respect et à encourager la coopération et le dialogue internationaux.

Incontestablement, dans ce domaine, l'Europe a fait front commun. D'ailleurs, l'accord général sur le commerce des services (GATS de 1994) a reconnu aux Etats la faculté de déroger aux règles de l'accès au marché au motif de la protection des données personnelles.

Les développements d'Internet, tout particulièrement celui du commerce électronique, ont d'ailleurs conféré à la question de la protection des données une place prépondérante dans les discussions internationales.

Dès 1996, la Maison Blanche a diffusé un document intitulé *Aframework for Global Electronic Commerce* qui témoignait d'une certaines avancée des positions américaines dans ce domaine. Ce document affirme en effet le « besoin de définir un environnement juridique transparent et harmonisé » notamment dans le domaine de la vie privée et consacre plusieurs droits fondamentaux de la protection des données qui nous sont, en Europe, familiers. Cette question est évoquée dans d'autres enceintes telles que l'Organisation mondiale du commerce.

La conférence du « projet pilote du *G7* sur le commerce électronique » qui s'est tenue à Bonn les 7 et 9 avril 1997 s'est conclue par une déclaration ministérielle sur les réseaux globaux de l'information valant engagement sur plusieurs principes de protection des données. Depuis lors, l'Union européenne et les États-Unis se sont accordés sur une déclaration commune relative au commerce électronique, le 5 décembre 1997. Enfin, l'OCDE qui avait adopté en 1980 des lignes directrices en matière de protection des données se montre tout particulièrement active sur la question du commerce électronique.

Ce foisonnement d'initiatives ou de déclaration d'intention ne saurait masquer l'essentiel : la différence d'approche, entre notamment l'administration américaine et les pays européens, demeure encore considérable.

L'administration américaine préfère en effet plutôt que l'adoption de règles homogènes dotées d'effets juridiques, le recours à des mécanismes

d'autorégulation qui seraient organisés par les professionnels eux-mêmes (code de conduite, code de déontologie). La pression de l'Europe et celle de nombreuses associations d'internautes se trouvent cependant à l'origine d'un relatif « durcissement » des positions de l'administration Clinton à l'égard des opérateurs du secteur privé. Aussi, l'administration américaine insiste désormais sur la nécessité que des voies de recours soient organisées par les professionnels afin de mettre en mesure les consommateurs, les internautes et les citoyens de faire valoir leurs droits et tout particulièrement leurs droits à réparation d'un éventuel préjudice. En outre, l'administration fédérale fait valoir que si les mesures prises par les professionnels n'étaient pas suffisantes, des dispositions législatives pourraient être adoptées, l'argument valant, aux États-Unis d'Amérique, incitation à agir, voire menace.

C'est dans ces conditions que les plus grands opérateurs américains sur le réseau s'efforcent de rechercher des solutions d'ordre technique afin de convaincre l'Europe qu'elles pourraient satisfaire à l'exigence du niveau adéquat de protection.

Un projet actuellement conduit par le Consortium 3 W, créé à l'initiative du MIT, avec l'INRIA (France) et l'université de Keio (Japon) et regroupant les principaux industriels d'Internet, illustre cette approche.

Ce projet repose sur les principes suivants : les sites devraient déterminer et rendre publique leur « pratique » en matière de protection de données personnelles ; les internautes pourraient intégrer dans les logiciels de navigation qu'ils utilisent leurs exigences dans ce domaine de sorte que ces logiciels puissent comparer automatiquement les exigences des utilisateurs aux garanties offertes par les sites en matière de protection des données : ainsi, des données personnelles ne seraient transmises que lorsque le site offrirait des garanties conformes aux exigences des utilisateurs.

Au-delà des nombreuses imperfections techniques de ce projet, à l'expertise duquel la CNIL a participé aux côtés d'autres autorités de protection de données, l'influence de cette position sur le débat en cours relatif au « niveau adéquat » de protection pourrait être déterminante, dès que la version des navigateurs diffusés par l'industrie américaine inclura cette fonctionnalité. L'existence de ce produit technique constituera en effet, à l'échelle mondiale du commerce électronique sur Internet, un puissant moyen de diffusion du modèle américain de la contractualisation de la protection des données. Or, il est essentiel de percevoir que ce modèle américain repose sur une philosophie tout à fait différente de celle qui inspire les principes européens de protection des données :

- il abandonne la protection des données à un « arrangement » entre le site et l'internaute, arrangement considéré comme loyal et suffisant dès lors qu'une claire et exacte information des internautes est faite selon l'adage américain « informer et choisir » « *notice and choice » ;*
- il repose sur le principe que la protection des données se limite à une relation de nature contractuelle entre l'internaute et le site quand, en Europe, la réflexion

sur la protection des données porte également sur les stocks des données qui sont constitués, sur leur durée de conservation et sur leur accessibilité à des tiers, tels que la police judiciaire, les autorités en charge de missions relevant de la sûreté de l'État, etc. ;

- il rend caduques pour Internet les règles du droit national applicable, telles qu'elles sont définies par la directive européenne quand le site est situé sur le territoire d'un Etat tiers ; en effet, ce ne seront pas alors les règles d'ordre public des législations de protection des données des pays européens qui régiront la matière mais « l'arrangement » passé entre le site et l'internaute européen ;
- enfin, le projet du consortium 3W prévoit qu'en cas de refus de l'internaute de transmettre des données personnelles à un site qui ne satisferait pas à ces exigences en la matière, des ristournes ou rabais lui seront proposés pour l'inciter à consentir à la transmission de ses données personnelles.

Ce projet manifeste aisément les limites des solutions qui reposeraient sur le choix individuel de l'internaute ou la « liberté » de contracter. Ce ne sont plus alors des données librement échangées qui transitent sur le réseau, il s'agit bien davantage de données extorquées à l'internaute, qui aura, sous l'effet de la sollicitation, abandonné le niveau de protection auquel il a droit.

Aussi, les autorités européennes de protection des données sont-elles en l'état réservées sur le caractère satisfaisant de cette solution.

En revanche, sur d'autres sujets, notamment les *cookies,* les opérateurs ont pu, sous la pression des utilisateurs et des recommandations faites par les autorités de protection des données dans le monde, proposer des solutions techniques satisfaisantes qui permettent à l'internaute d'être avisé de l'existence d'un *cookie,* d'en refuser l'inscription sur le disque dur de son ordinateur, au cas par cas d'abord — ce qui présentait cependant l'inconvénient de ralentir considérablement la navigation sur Internet — de manière générale ensuite, ce qui constitue une solution bien plus satisfaisante.

À ce stade de sa réflexion, nourrie de l'expérience et de l'étroite collaboration qu'elle entretient avec les autres autorités européennes ou internationales de protection des données, la CNIL a fait part, au Gouvernement français qui l'avait consultée sur ce point, que les principes de protection des données consignés dans la directive européenne et le dispositif que prévoit ce texte en matière de flux transfrontières devaient être soutenus et préservés lors des discussions internationales en cours sur le sujet.

Au demeurant, toute faiblesse dans la négociation serait de nature à créer une grave distorsion de concurrence au détriment des entreprises établies en Europe qui elles sont en tout état de cause astreintes à respecter les normes juridiques applicables en matière de protection des données et doivent pouvoir développer leurs activités dans des conditions équitables de concurrence vis-à-vis des pays tiers.

Quelle que soit la difficulté du sujet et sans nier l'intérêt, voire la nécessité, de rechercher des solutions adaptées aux flux transfrontières ou à la

circulation des données personnelles sur le réseau, l'Europe paraît faire front, avec imagination mais détermination. Il convient de rappeler qu'à l'occasion de leur dernière conférence qui s'est réunie à Dublin les 23 et 24 avril 1998, les commissaires européens à la protection des données ont adopté une résolution rappelant « que les règles de la protection des données personnelles, telles qu'elles résultent de la réglementation européenne, s'appliquent intégralement, selon des modalités appropriées, à toutes les informations fournies au réseau Internet ou transmises à ce réseau par quelque moyen, logiciel ou technique que ce soit ».

L'Europe a imposé dans diverses négociations internationales l'exception culturelle. Le temps est venu de gagner l'exception de la protection des données.

Troisième partie

L'INTERVENTION DE LA CNIL DANS LES PRINCIPAUX SECTEURS D'ACTIVITÉ

Chapitre 1

COLLECTIVITÉS LOCALES

VIE PUBLIQUE

I. LA VIE MUNICIPALE

Au titre de leurs attributions, les communes sont naturellement conduites à détenir, ou simplement à connaître, de nombreuses informations sur leurs administrés. Elles sont parfois tentées de les utiliser à des fins dont certaines sont légitimes — telles par exemple l'envoi à la population d'informations sur la vie municipale — mais dont d'autres, sont plus contestables : il en est ainsi de l'utilisation, à des fins de propagande politique, des fichiers de gestion communale. La Commission est ainsi régulièrement interrogée par des services municipaux ou par des particuliers sur les conditions dans lesquelles une mairie peut ou non collecter et utiliser des données nominatives sur ses administrés, peut ou non répondre à des demandes de renseignements qui lui sont présentées par telle ou telle administration ou organisme extérieur.

Pour répondre à de telles interrogations, la CNIL a élaboré un guide pratique « Collectivités locales, informatique et libertés » qui recense, sur la base des avis, recommandations et conseils que la CNIL a pu émettre depuis vingt ans dans ce domaine, les réponses aux questions les plus courantes (*cf. supra 1re* partie, chapitre 1).

A. La communication aux maires de données socio-économiques

1) LES LISTES DE DEMANDEURS D'EMPLOI

Les collectivités locales jouent un rôle de plus en plus important dans la lutte contre le chômage et la précarité. Elles peuvent en effet recevoir des offres

d'emploi ou encore effectuer des opérations de placement en faveur de leurs administrés. Les articles L. 31 1-11 et R. 311 -5-4 du code du travail ont d'ailleurs prévu que les maires, dans la perspective d'opérations de placement ou pour la détermination d'avantages sociaux auxquels peuvent prétendre leurs administrés, ont la possibilité d'obtenir la liste des demandeurs d'emplois domiciliés dans leur commune, c'est-à-dire les noms, prénoms et adresses des personnes inscrites à l'ANPE ainsi que, le cas échéant, la mention qu'un revenu de remplacement est versé.

Dans un souci d'efficacité de l'action locale des maires en faveur de l'emploi, la CNIL, saisie par le ministre du Travail et des Affaires sociales d'un projet de décret modifiant l'article R. 311 -5-4 du code du travail, a admis que la qualification professionnelle des demandeurs d'emplois puisse également être transmise aux maires par l'ANPE. Il est à noter qu'à la date de rédaction du présent rapport ce décret n'a toujours pas été publié.

Toutefois, la Commission a pu constater que la communication aux maires de la liste des demandeurs d'emplois suscitait des interrogations de la part d'administrés concernés, surpris que le maire de leur commune puisse avoir connaissance de leur situation personnelle ; de même, la Commission a pu relever quelques cas d'utilisation de ces informations à des fins sans rapport avec des missions de placement.

Aussi, la CNIL demande que les demandeurs d'emplois soient clairement informés par l'ANPE de ces transmissions d'informations et de leur finalité, et recommande aux services municipaux de préciser, dès les premiers courriers adressés à un demandeur d'emploi, l'origine des informations utilisées et le fondement légal de cette communication.

En outre, la CNIL rappelle que toute utilisation de ces informations à d'autres fins, notamment à des fins politiques, est proscrite, le courrier adressé par une mairie aux demandeurs d'emploi ne devant comporter aucune référence à une permanence électorale et aucun message à connotation politique.

2) LES DONNÉES RELATIVES AU RMI

La Commission a été saisie par un maire qui sollicitait son avis sur la possibilité de communiquer, à la demande de certains conseillers municipaux, la liste nominative des bénéficiaires du RMI de la commune ou, à défaut, un état statistique faisant notamment apparaître leur nationalité, sous la forme « Français, ressortissants de l'Union européenne, étrangers hors Union ».

La CNIL a indiqué qu'aux termes de la loi du 1er décembre 1988 modifiée, relative au revenu minimum d'insertion, seuls sont destinataires des informations nominatives, dans la limite de leurs attributions, les organismes instructeurs et les organismes payeurs, le représentant de l'État dans le département, le président du conseil général, le président de la commission locale

d'insertion ainsi que les présidents des centres communaux d'action sociale (CCAS) concernés.

Ainsi, dans la commune, seul le maire, en tant que président du CCAS tenu au respect du secret professionnel, peut être destinataire de la liste des bénéficiaires du RMI, les conseillers municipaux ne pouvant pas légalement l'être. En revanche, la transmission aux autres élus municipaux de données socio-démographiques concernant les bénéficiaires de la commune est possible dès lors que les statistiques produites ne permettent en aucune façon l'identification des personnes.

Enfin, la Commission rappelle que les informations nominatives concernant les bénéficiaires du RMI ne doivent pas être conservées sur support informatique au-delà d'un an après la sortie du dispositif RMI et de six mois en cas de refus de l'aide opposé par le préfet.

B. L'utilisation par des tiers de données de l'état civil

Depuis quelques années, les services d'état civil se sont fortement informatisés dans le souci de mieux répondre aux demandes des administrés ou des administrations. En pratique, les mairies recourent principalement à deux catégories d'applications informatiques : d'une part, des applications visant à la tenue des registres proprement dits, à l'édition des tables annuelles et décennales d'état civil et à la transmission des informations d'état civil à certaines administrations, en particulier l'INSEE ; d'autre part, des applications visant à la rédaction assistée par ordinateur des actes d'état civil et à une édition d'extraits et de copies des actes. Dans tous les cas, la Commission rappelle que les administrés doivent être informés, notamment par voie d'affichage, de cette informatisation.

S'il convient de relever que les copies d'actes de décès, de même que les extraits d'actes de naissance et de mariage, peuvent être délivrées à toute personne qui en fait la demande, toutes les informations nominatives nécessaires à l'inscription d'un acte sur le registre d'état civil ne peuvent être utilisées que pour l'accomplissement des missions dont sont investis les maires en leur qualité d'officier d'état civil et ne doivent être communiquées qu'aux destinataires habilités à en connaître (procureurs de la république, INSEE, services de protection maternelle et infantile...). A titre d'exemple, des données telles que l'adresse ou encore la profession, qui ne figurent pas sur les extraits d'actes, ne peuvent en aucun cas être divulguées à des tiers.

L'attention de la Commission est régulièrement appelée sur les pratiques de certaines municipalités consistant à transmettre aux journaux locaux ou à des organismes privés opérant par voie de prospection commerciale, la liste des naissances ou mariages intervenus dans la commune avec la mention de l'adresse des jeunes mariés ou des parents. Cette pratique suscite auprès de la Commission de nombreuses plaintes de parents ou de jeunes mariés soucieux de protéger l'intimité de leur vie privée.

Le décret du 3 août 1962 modifiant certaines règles relatives aux actes d'état civil établit clairement que, sauf autorisation du procureur de la République, l'adresse des personnes enregistrées à l'état civil ne peut être communiquée qu'aux seuls destinataires des copies intégrales des actes de naissance, de reconnaissance ou de mariage, à savoir : l'intéressé lui-même, ses ascendants et descendants directs, son conjoint, son représentant légal et le procureur de la République. La Commission rappelle donc régulièrement aux mairies leurs obligations en matière de communication d'informations.

La Commission a été saisie cette année d'une plainte sur une affaire très douloureuse qui révèle la nécessité de prendre des précautions. En l'espèce le plaignant, père d'un enfant décédé le jour même de sa naissance, avait reçu un courrier d'un institut universitaire de psychologie lui proposant que son enfant puisse faire l'objet d'une étude menée sur le comportement des nourrissons. Particulièrement choqué par cette démarche, le parent a saisi la CNIL.

En fait, il est apparu que l'organisme de recherche avait été autorisé par le procureur de la République, conformément au décret du 3 août 1962 modifié et relatif en outre à la publicité des actes d'état civil, à consulter et à se voir délivrer les copies intégrales des actes de naissance de cette mairie. En pratique, les services de la mairie transmettaient donc régulièrement à l'institut de recherche la liste nominative des nouveau-nés. La précaution n'avait pas été prise par la mairie de rapprocher les listes des naissances des listes de décès.

La Commission a saisi la mairie concernée, afin que soit instaurée une procédure permettant d'éviter qu'à l'avenir des données relatives à des nouveau-nés décédés ne soient transmises à l'institut de psychologie, ce qui fut fait, le logiciel servant à l'extraction des données d'état civil ayant été modifié afin que seuls les nom et adresse des parents d'enfants dont l'acte de naissance, à la date de la demande, ne comporte pas une mention de décès en marge, soient communiqués à l'Institut.

En outre, la CNIL est intervenue auprès de l'Institut de recherche afin que la lettre adressée aux parents soit complétée par l'indication de l'origine des fichiers utilisés et par une mention informant les parents de leur possibilité de se faire radier du fichier d'adresses détenu par l'Institut, fichier qui dans tous les cas est épuré trois mois après l'envoi du courrier aux parents.

C. La vérification sur place auprès de la direction du logement de la ville de Paris

La mairie du III^{e} arrondissement de Paris a saisi la CNIL d'un dossier de refus d'attribution d'un logement social à une personne qui faisait apparaître, sur un document émanant de la direction de la construction et du logement, la mention « Sénégal » alors même que, de surcroît, le demandeur était de nationalité française.

La CNIL a décidé, par délibération n° 96-106 du 3 décembre 1996, de procéder à une mission de vérification sur place à la direction de la construction et du logement désormais dénommée direction du logement et de l'habitat de la mairie de Paris.

Ces investigations ont permis de constater que si le dossier papier du demandeur indiquait bien sa date et son lieu de naissance, informations qui avaient été régulièrement portées à la connaissance de la direction du logement et de l'habitat au titre des éléments d'état civil, le fichier informatique de gestion des candidatures faisait seulement apparaître au regard de ces rubriques la mention « pays étranger ». L'indication « Sénégal » figurait quant à elle sur un document édité par la mairie de Paris et transmis à la direction du logement. Cette information, régulièrement recueillie dans la mesure où elle identifie le pays de naissance, n'avait pas été portée à la connaissance de la société gestionnaire des logements, laquelle a motivé son refus d'attribuer le logement par l'inadéquation entre la superficie de l'appartement et la taille de la famille, dont la demande au demeurant était soutenue tant par la mairie d'arrondissement que par la mairie de Paris.

En définitive, la CNIL a estimé qu'il n'y avait pas eu méconnaissance de la loi du 6 janvier 1978. La Commission a toutefois rappelé que l'indication du pays d'origine, bien que cette information résulte immanquablement de l'état civil de la personne, ne fait pas en tant que telle l'objet d'un traitement informatique particulier qui pourrait permettre d'effectuer des tris, notamment entre français, sur ce critère ; la Commission a aussi souligné la nécessité que le lieu de naissance n'apparaisse que dans la rubrique conçue à cet effet. En ce sens, il a été demandé à la mairie de Paris de s'assurer que son application bureautique enregistrait des informations strictement conformes à celles contenues dans l'application de la direction du logement et de l'habitat, dont elle ne constitue que l'accessoire.

Délibération n° 97-026 du 1er avril 1997 relative à la visite sur place effectuée le 7 janvier 1997 à la direction de la construction et du logement de la mairie de Paris

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 le règlement intérieur de la Commission, notamment ses articles *55* à *57 ;*

Vu la délibération n° 96-106 du 3 décembre 1996 décidant une mission de vérification sur place auprès de la mairie de Paris, direction de la construction et du logement ;

Vu le compte rendu de la mission de vérification sur place effectuée le 7 janvier 1997 ;

Vu les observations formulées par le directeur adjoint du cabinet du maire de Paris dans un courrier daté du 14 mars 1997 ;

Après avoir entendu Madame Isabelle Jaulin, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Considérant qu'à la suite du refus de logement qui avait été opposé à un demandeur de logement social, Monsieur M., dont la candidature avait été présentée par le maire du III^{e} arrondissement, ce dernier a saisi la Commission par un courrier du 25 novembre 1996 auquel étaient jointes une fiche émanant de la direction de la construction et du logement (DCL) de la mairie de Paris et une fiche paraissant émaner du cabinet du maire de Paris qui comportait au regard de la rubrique « numéro d'inscription DCL », la mention « Sénégal » alors même que le demandeur était de nationalité française ;

Considérant que par délibération n° 96-106 du 3 décembre 1996, la Commission a décidé d'effectuer une mission de vérification sur place auprès de la mairie de Paris, direction de la construction et du logement ;

Considérant que cette mission a été effectuée le 7 janvier 1997 à la direction de la construction et du logement de la mairie de Paris et a été complétée par l'envoi de courriers sollicitant des compléments d'information, l'un, le 17 janvier 1997, au directeur du cabinet du maire de Paris, l'autre, le 20 janvier 1997, au sous-directeur de la direction du logement et de l'habitat ; que les réponses à ces courriers sont parvenues à la Commission le 31 janvier 1997 ;

Considérant qu'il résulte des investigations accomplies que la direction de la construction et du logement de la mairie de Paris — désormais dénommée direction du logement et de l'habitat— dispose, depuis 1982 d'un traitement automatisé d'informations nominatives régulièrement déclaré à la CNIL sous la finalité « gestion du fichier des candidats à l'attribution des logements sociaux » ; que le traitement prévoyait notamment, au titre des informations collectées, la nationalité et le lieu de naissance des demandeurs ; qu'un récépissé a été délivré à la date du 25 janvier 1983 ;

Considérant que l'information relative au pays de naissance du demandeur a régulièrement été portée à la connaissance des services de la direction de la construction et du logement et du cabinet du maire de Paris au titre des éléments de l'état civil (date et lieu de naissance) ; que cette information figure en clair dans le dossier papier de candidature de Monsieur M. ; qu'elle a été enregistrée sous la rubrique date et lieu de naissance dans le traitement automatisé mis en oeuvre par la DCL sous l'indication « pays étranger » ; qu'une consultation sur place de ce traitement a en effet permis de constater que le lieu de naissance du demandeur est enregistré sans codification particulière ; qu'ainsi figure parfois à cette rubrique l'indication de la commune seule ou celle de la commune et du pays ou celle du seul pays sans la commune ou encore la seule mention « pays étranger » ;

Considérant que l'indication « Sénégal » figurait sur un document édité par l'application bureautique du cabinet du maire et transmis à la direction du logement et de l'habitat ; que cette indication correspond à une information qui pouvait être régulièrement collectée au titre des éléments de l'état civil qui inclut le lieu de naissance, et qu'elle n'a pas eu pour effet de porter à la connaissance de quiconque une information qui ne devait pas l'être ; qu'enfin le document papier transmis par la direction du logement et de l'habitat à la société gestionnaire à laquelle la candidature de Monsieur M.

a été proposée ne comportait d'autres indications sur le demandeur que son nom, son adresse et son numéro de téléphone ; qu'en outre la société gestionnaire n'a statué sur cette candidature qu'au vu des éléments directement recueillis par elle auprès du candidat, cette société ne disposant pas du dossier de candidature déposé auprès de la mairie de Paris, ni de documents internes à la Ville de Paris, ni d'un accès quelconque au traitement automatisé de la direction du logement et de l'habitat ;

Considérant que l'apposition, sur la fiche-navette adressée par le cabinet du maire à la direction du logement et de l'habitat, de l'indication « Sénégal » au regard de la rubrique « n° d'inscription DCL » résulte du fait qu'à l'époque de l'inscription du candidat, le cabinet du maire, auquel s'adressent parfois directement les candidats à un logement, saisissait sur son application bureautique de type traitement de texte, à cet emplacement, le pays de naissance des demandeurs ; que depuis 1994, cette information ne revêtant pas d'utilité particulière a été remplacée par le numéro d'inscription attribué par la DCL ; que la mise à jour qui a alors été opérée sur cette rubrique en substituant le numéro DCL à l'indication du pays de naissance n'a pas été exhaustive ; que dans certains cas, et tout particulièrement celui des candidatures anciennes n'ayant pas fait l'objet de propositions d'attributions de logements depuis 1994, l'indication du pays de naissance a pu subsister et peut alors se trouver imprimée sur les fiches de proposition de logement que le cabinet du maire adresse à la direction du logement et de l'habitat ; que tel a été le cas de Monsieur M. qui avait présenté sa candidature au cabinet du maire de Paris en 1981 ;

Considérant dès lors que la mention de cette information au regard de la rubrique « n° DCL », qui pouvait légitimement en première analyse, paraître surprenante, ne caractérise pas une méconnaissance de la loi du 6 janvier 1978 ;

Considérant qu'il y a lieu de rappeler que la collecte et l'enregistrement dans les traitements de gestion des attributions de logements sociaux de l'état civil, date et lieu de naissance y compris, et de la nationalité des personnes sont considérés comme pertinents au regard de la finalité de ces traitements ;

Considérant cependant que la Commission recommande généralement que l'indication du pays d'origine, bien que cette information résulte immanquablement de l'état civil de la personne, ne fasse pas, en tant que telle, l'objet d'un traitement informatique particulier qui pourrait permettre d'effectuer des tris, notamment entre Français sur ce critère ; que si tel n'a pas été le cas en l'espèce, il convient de recommander que la mise à jour de l'application bureautique dont dispose le cabinet du maire de Paris dans le cadre du traitement régulièrement déclaré de gestion du fichier des candidats à l'attribution des logements sociaux, soit assurée de sorte que n'apparaisse plus dans une rubrique autre que celle réservée à l'état civil le lieu de naissance des personnes concernées ; qu'en outre l'indication du lieu de naissance des demandeurs devrait faire l'objet d'une harmonisation afin que soit évité l'utilisation du terme générique « pays étranger » ;

Recommande à la mairie de Paris de s'assurer de la mise à jour des informations de sorte qu'en aucun cas les informations relatives aux demandeurs n'apparaissent dans son application bureautique sous une autre forme que celle sous laquelle elles sont enregistrées dans l'application de la DCL ; que l'indication du pays de naissance des demandeurs de logement fasse l'objet d'une harmonisation.

II. LES NOUVEAUX OUTILS DE LA CITOYENNETÉ

A. L'inscription automatique sur les listes électorales

À la suite de l'engagement du Gouvernement que l'inscription de chaque citoyen sur les listes électorales soit rendue automatique l'année de sa majorité, la CNIL a été saisie pour avis d'un avant-projet de loi modifiant les articles L. 11 et L. 17 du code électoral. Cette saisine de la CNIL se justifiait pleinement dans la mesure où la mise en œuvre de ce projet supposait un recensement de la population concernée reposant pour l'essentiel sur le recours à des fichiers ou des traitements automatisés dans lesquels des personnes de cette tranche d'âge sont susceptibles de figurer.

La note d'observations que la CNIL a alors adressé au Gouvernement recommandait que plusieurs conditions devraient être respectées afin que le dispositif arrêté par les pouvoirs publics soit conforme aux règles fondamentales de la protection des données. C'est ainsi que la CNIL a notamment préconisé, d'une part, que les commissions administratives chargées d'établir la liste électorale ne disposent pas d'un droit de regard sur l'ensemble des informations contenues dans des fichiers détenus par des tiers, que ces informations se rapportent à des personnes non concernées par l'avant-projet de loi ou qu'elles soient dépourvues d'intérêt pour l'objectif considéré ; elle a d'autre part demandé que soit proscrit le recours à des fichiers dont la finalité même caractérise une situation personnelle ou un choix des intéressés (fichiers de personnes insolvables, de membres d'associations, etc.).

Ainsi, la CNIL a-t-elle recommandé que tous les fichiers mis en œuvre dans le secteur privé soient exclus de la procédure de recensement des jeunes, que le ou les fichiers publics qui pourraient être utilisés aux fins de recensement de la population concernée soient parfaitement identifiés et limitativement énumérés, soit par la loi elle-même, soit par un décret pris en Conseil d'État après avis de la CNIL, que le choix soit fait plutôt que d'abandonner l'initiative du recensement aux commissions administratives, d'imposer aux responsables de certains fichiers identifiés de communiquer d'office aux commissions administratives les seules informations utiles, à savoir les nom, prénoms, adresse, date et lieu de naissance et qu'à l'issue des opérations d'inscription sur les listes électorales, c'est-à-dire lors de la clôture définitive des listes, l'ensemble des informations qui auraient été transmises aux commissions administratives soient, quelle qu'ait été la suite réservée, détruites sous sa seule autorité. À l'issue de cette consultation, un texte s'inspirant largement des suggestions de la Commission a été soumis au Parlement, lequel a adopté pour l'inscription d'office des personnes atteignant l'âge de 18 ans un dispositif reposant sur la communication systématique par les responsables des fichiers du recensement établi en application du code du service national d'une part, et des organismes servant les prestations de base des régimes d'assurance maladie d'autre part, des seules

informations suivantes : nom, prénoms, nationalité, date de naissance et adresse. Ces informations sont communiquées aux commissions administratives existant dans chaque bureau de vote, par l'intermédiaire de l'INSEE. La loi prévoit enfin, comme l'avait suggéré la Commission, que les informations transmises aux commissions administratives soient détruites à l'expiration des délais de recours ou, le cas échéant, après l'intervention de la décision définitive.

Pour le lancement de ces procédures d'inscription automatique, la CNIL a été saisie par l'INSEE d'un projet d'arrêté portant création d'un fichier central de proposition d'inscription d'office sur les listes électorales et d'un projet de décret en Conseil d'État, pris en application de l'article 18 de la loi du 6 janvier 1978, autorisant l'utilisation du répertoire national d'identification des personnes physiques (RNIPP) pour la gestion de ce fichier.

En effet, au-delà de sa finalité de recensement des personnes remplissant la condition d'âge requise par le code électoral, le fichier central doit permettre :
- de certifier l'identité des personnes ainsi que l'absence de mention de décès par confrontation avec le RNIPP ;
- de contrôler la capacité électorale auprès du fichier général des électeurs et électrices ;
- de transmettre aux maires les listes nominatives de proposition d'inscription d'office par commune ;
- de procéder à l'inscription des nouveaux électeurs au fichier général des électeurs et électrices.

La CNIL a donné un avis favorable aux deux projets d'actes réglementaires présentés, et elle a demandé à être informée par l'INSEE des modalités de mise en oeuvre et de fonctionnement du fichier central de proposition d'inscription d'office sur les listes électorales.

Délibération n° 97-088 du 18 novembre 1997 portant avis sur :
— Le projet d'arrêté, présenté par l'INSEE, portant création du fichier central de proposition d'inscription d'office sur les listes électorales
— Le projet de décret en Conseil d'État, pris en application des dispositions de l'article 18 de la loi du 6 janvier 1978 autorisant l'utilisation du répertoire national d'identification des personnes physiques pour la gestion du fichier central de proposition d'inscription d'office sur les listes électorales
(Demande d'avis n° 549 627)

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, notamment ses articles 15 et 18 ;

Vu le code électoral, notamment les articles L. 11-1, L. 17-1, L. 37 et R. 20 à 22 ; Vu le code du service national ; Vu le code de la sécurité sociale ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres 1er à IV et VI de la loi du 6 janvier 1978 susvisée ;

Vu le décret n° 83-101 du 15 février 1983 autorisant l'utilisation du répertoire national d'identification des personnes physiques en vue de la tenue du fichier général des électeurs et électrices ;

Vu le décret n° 85-420 du 3 avril 1985 relatif à l'utilisation du répertoire national d'identification des personnes physiques par des organismes de sécurité sociale et de prévoyance ;

Vu le projet d'arrêté interministériel portant création du fichier central de proposition d'inscription d'office sur les listes électorales ;

Vu le projet de décret en Conseil d'État pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'utilisation du répertoire national d'identification des personnes physiques pour la gestion du fichier central de proposition d'inscription d'office sur les listes électorales ;

Après avoir entendu Messieurs Michel Bernard et Charles Renard, commissaires en leur rapport, ainsi que Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations.

Sur le projet d'arrêté portant création du fichier central de proposition d'inscription d'office sur les listes électorales

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'un traitement automatisé d'informations nominatives dénommé fichier central de proposition d'inscription d'office sur les listes électorales ;

Considérant que, en application de l'article L. 11-1 du code électoral, le traitement considéré doit permettre l'inscription d'office sur la liste électorale de leur domicile réel des personnes qui atteignent l'âge de 1 8 ans entre la date de la dernière clôture définitive des listes électorales et le 28 ou 29 février de l'année suivante ;

Considérant que l'INSEE est chargé de rassembler les informations nominatives concernant les personnes remplissant la condition d'âge fixée par l'article L. 11-1 du code électoral ; que ces informations lui seront transmises, d'une part par les autorités responsables du fichier du recensement établi en application du code du service national et d'autre part, par les organismes servant les prestations de base des régimes obligatoires d'assurance maladie ;

Considérant que l'INSEE, dans un premier temps, certifiera, par confrontation avec le répertoire national d'identification des personnes physiques (RNIPP) l'état civil des personnes concernées et vérifiera l'absence de mention de décès ; qu'il vérifiera dans un second temps dans le fichier général des électeurs et électrices l'absence d'inscription volontaire préalable et la capacité juridique des intéressés ;

Considérant que le fichier central de proposition d'inscription d'office sur les listes électorales comportera pour chaque personne concernée les données suivantes : nom patronymique, nom d'usage le cas échéant, prénoms, date et lieu de naissance, sexe, numéro d'inscription au répertoire, identifiant de l'organisme source de l'information, adresse, capacité électorale, éventuellement date de décès, date et lieu d'inscription éventuelle ;

Considérant que, tous les contrôles ayant été effectués, l'INSEE constituera, par commune, des listes nominatives de proposition d'inscription d'office ; que ces listes seront adressées, sur support papier ou informatique, aux maires, pour examen et décision d'inscription d'office par la Commission administrative compétente, conformément aux dispositions de l'article L. 17-1 du code électoral ;

Considérant qu'il y a lieu de rappeler que l'article L. 17-1 du code électoral prévoit que les Commissions administratives sont les destinataires de ces informations qu'elles doivent faire détruire soit à l'expiration des délais des recours prévus aux articles L. 20 et L. 25 du code électoral soit, dans le cas où un recours a été introduit, après l'intervention de la décision définitive ;

Considérant que les données nominatives figurant sur les listes seront relatives au nom patronymique, nom d'usage le cas échéant, prénoms, date et lieu de naissance, sexe, identifiant de l'organisme source de l'information, adresse ;

Considérant que les mairies retourneront à l'INSEE les listes mentionnant la décision de la Commission administrative ; que dès réception de ces listes, l'INSEE procédera à l'inscription des intéressés sur le fichier général des électeurs et électrices ;

Considérant que les informations nominatives seront conservées dans le fichier central de proposition d'inscription d'office sur les listes électorales dans un délai de trois mois à compter de la réception des listes retournées par les communes ; qu'en tout état de cause, la durée totale de conservation des données n'excédera pas dix-huit mois à compter de la réception initiale ;

Considérant que les personnes concernées pourront exercer le droit d'accès qui leur est reconnu par l'article 34 de la loi du 6 janvier 1978 auprès de la direction régionale de l'INSEE des Pays de la Loire ;

Sur le projet de décret en Conseil d'État pris en application de l'article 18 de la loi du 6 janvier 1978

Considérant que l'INSEE a saisi la Commission d'un projet de décret qui a pour objet de l'autoriser en application de l'article 18 de la loi du 6 janvier 1978 à utiliser le répertoire national d'identification des personnes physiques pour la gestion du fichier central de proposition d'inscription d'office sur les listes électorales ;

Considérant que cette utilisation du répertoire et du numéro d'inscription au répertoire n'a d'autre but que de certifier les états civils des personnes inscrites dans le fichier central de proposition d'inscription d'office sur les listes électorales, en vue de leur inscription sur le fichier général des électeurs et électrices, tenu par l'INSEE et d'éliminer les personnes décédées ;

Considérant que l'article 2 du projet de décret prévoit de compléter le décret n° 85-420 du 3 avril 1985 susvisé par un article 2 bis relatif à la transmis-

sion à l'INSEE du numéro d'inscription au répertoire (NIR) pour la gestion du fichier central de proposition d'inscription d'office sur les listes électorales ;

Considérant que cette transmission du NIR à l'INSEE est justifiée par la finalité spécifique de l'opération ; qu'elle ne soulève pas de difficulté particulière ;

Considérant que l'article 3-1 du projet de décret renvoie à un arrêté interministériel valant acte réglementaire au sens de l'article 15 de la loi du 6 janvier 1978, les modalités de transmission des données par les caisses d'assurance maladie au fichier central de proposition d'inscription d'office sur les listes électorales de l'INSEE ;

Considérant que cette disposition n'a pas pour effet de modifier la procédure prévue par l'article 15 de la loi du *6* janvier 1978 ;

Considérant enfin que l'article 3-II du projet de décret a pour effet de dispenser les organismes d'assurance maladie d'adresser à la CNIL de nouveaux actes réglementaires incluant l'INSEE au titre des destinataires de certaines informations figurant dans leurs traitements de gestion ; que cette disposition a pour objet de simplifier les démarches devant être accomplies auprès de la CNIL ; que si elle déroge à l'article 12 du décret n° 78-774 du 17 juillet 1978, elle ne méconnaît ni l'article 15 de la loi du 6 janvier 1978, ni aucune autre disposition de cette loi ;

Émet :

- **un avis favorable** au projet d'arrêté portant création du fichier central de proposition d'inscription d'office sur les listes électorales ;
- **un avis favorable** au projet de décret en Conseil d'État qui lui est soumis.

Demande à être informée par l'INSEE des modalités de mise en œuvre et de fonctionnement du fichier central de proposition d'inscription d'office sur les listes électorales.

B. Les pétitions par voie télématique

Une société a déclaré à la CNIL un service télématique, accessible par le 3615 « La Pétition », qui offre la possibilité de créer ou de soutenir des pétitions. Il s'agit en fait d'un « service » permettant de pétitionner par minitel comme on peut le faire, moins commodément sans doute, mais avec quelques garanties liées à la tradition, sur un trottoir, à la sortie d'une station de métro ou à la porte d'une usine.

Ce dossier soulevait diverses difficultés.

La première est liée aux conditions d'application de l'article 31 de la loi, les pétitions portant parfois sur des sujets de nature politique. Or l'article 31 de la loi du 6 janvier 1978 interdit, sauf accord exprès de l'intéressé, la collecte et la conservation de données nominatives qui font apparaître les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales, ou encore les mœurs des personnes. La Commission a considéré que l'exigence de l'accord exprès pouvait, en l'espèce, être considérée comme satisfaite dès lors que les usagers étaient informés de ce que leur

participation à la pétition était facultative et que, le cas échéant, leur soutien pourrait révéler directement ou indirectement, des données sensibles qui ne peuvent être recueillies qu'avec leur accord exprès. La CNIL a en outre précisé qu'il convenait d'indiquer sur une page écran obligatoirement consultée par les signataires ou les auteurs des pétitions, les conditions d'exercice des droits d'accès, de rectification et de suppression, ainsi que les destinataires des données nominatives.

La deuxième difficulté tenait aux risques d'usurpation d'identité de « mauvais plaisantins » que l'absence de signature et les conditions de moins grande publicité du soutien — chez soi, devant son minitel et non dans la rue en présence des organisateurs de la pétition — pouvaient laisser redouter.

Toutefois, le dispositif « 3615 La pétition » est encadré par des procédures d'authentification du pétitionnaire, qui dispose d'ailleurs d'un délai de *71* heures pour confirmer par courrier recommandé avec accusé de réception sa pétition ; à défaut, la société qui diffuse le service se réserve le droit de la supprimer. En tout état de cause, le texte d'une pétition doit respecter l'ordre public et les lois françaises. La Commission a souhaité appeler l'attention de la société gestionnaire de ce service sur les risques réels d'usurpation d'identité et sur la nécessité d'avertir les usagers du service de la possibilité d'une vérification auprès des personnes enregistrées comme pétitionnaires du soutien qu'elles apportent à la pétition.

Chapitre 2

FISCALITÉ

I. LA DIFFUSION DES STATISTIQUES FISCALES

La direction générale des impôts (DGI) a soumis à la CNIL un projet d'instruction rassemblant les principes que doivent respecter les directions régionales et départementales des services fiscaux pour la diffusion d'informations fiscales à caractère statistique. Cette instruction a été élaborée à la lumière des différents avis rendus par la Commission depuis 1991 sur les modalités de cession ou de transmission de données fiscales anonymes à des organismes producteurs de statistiques non régis par la loi n° 51-711 du 7 juin 1951.

L'application du principe de la libre diffusion des données à caractère statistique impose que soient déterminés les critères sur la base desquels on considérera qu'une information a perdu tout caractère nominatif. Il s'agit en effet de garantir le respect tant du secret statistique que de l'article 29 de la loi du 6 janvier 1978, aux termes duquel toute communication à des tiers non autorisés de données nominatives est interdite.

Plusieurs critères doivent être définis :

— le premier concerne le nombre minimum de personnes concernées par une information statistique pour que celle-ci ne puisse plus être considérée comme nominative, même de façon indirecte. En effet, pour pouvoir être diffusée, une information doit se rapporter à des personnes dont l'identification a été rendue impossible. Cette condition n'est pas remplie si l'information ne se rapporte qu'à une seule personne, même si celle-ci n'est pas nommée. De la même manière, l'information ne doit pas concerner une population trop réduite, sous peine de rester indirectement nominative. Le seuil en deçà duquel l'information reste

nominative doit être fixé en tenant compte du nombre de variables utilisées, de leur degré de précision (notamment en ce qui concerne les identifiants géographiques retenus) et de leur degré de rareté ; il doit donc être adapté aux circonstances de l'espèce ;
- le deuxième critère concerne les populations non homogènes, au sein desquelles certaines unités de base représentent une part prépondérante de l'ensemble ainsi constitué. Dans de telles hypothèses, il faut définir la part maximale qu'une unité de base peut représenter au sein de la population observée au-delà de laquelle l'information perdrait tout caractère anonyme ;
- avec le troisième critère, il ne s'agit pas d'empêcher de retrouver la personne concernée par une information individuelle mais d'éviter qu'une donnée agrégée puisse constituer, sur la base d'une probabilité, un profil de zone caractérisant trop finement les individus ; cette approche conduit à déterminer des seuils minimum d'agrégation en deçà desquels les informations agrégées ne peuvent pas être diffusées.

La doctrine de la Commission sur ces questions, qui a principalement été élaborée à l'occasion de l'examen des conditions de diffusion des données issues du recensement général de la population et qui apparaît déjà, dans le secteur fiscal, à la lecture de précédentes délibérations (cf. 12e rapport, p. 191, 16e rapport, p. 149), s'inspire largement des règles appliquées par l'INSEE en matière de diffusion de données agrégées, dont les modalités varient selon qu'il s'agit de personnes physiques ou de personnes morales.

Certaines règles proposées par la DGI ont paru tout de suite satisfaisantes : les informations agrégées relatives à l'impôt sur le revenu, à la taxe d'habitation et à l'impôt de solidarité sur la fortune ne seront pas communiquées au public lorsqu'elles concerneront moins de onze unités — en l'espèce des foyers fiscaux —. De même, une donnée agrégée ne sera pas communiquée si elle se rapporte surtout à un élément « dominant », représentant plus de 85 % du montant agrégé. Les informations agrégées ne seront par principe communi-cables qu'au niveau de la région, du département ou de la commune, le seul niveau infra-communal envisagée étant l'arrondissement pour Paris, Lyon et Marseille. La mise en oeuvre, par les services informatiques de la DGI, d'un traitement informatique spécifique d'anonymisation des données devrait assurer l'application effective de ces règles avant toute communication d'informations à des tiers.

Dans son avis, la Commission s'est principalement montrée préoccupée par la faiblesse du niveau minimum d'agrégation retenu par le projet d'instruction pour l'ensemble des informations relatives à la fiscalité professionnelle — trois unités —, alors même que ces informations peuvent concerner des personnes physiques. Tel peut être le cas en matière de taxe professionnelle ou de TVA. Tel est toujours le cas pour les déclarations spécifiques consacrées à certaines catégories particulières de revenus professionnels qui sont rattachés, de plein droit ou sur option, au revenu net global d'un foyer fiscal et qui sont ainsi soumis à l'impôt sur le revenu.

En effet, le seuil de trois unités n'exclut pas toute identification des déclarants, et ce d'autant moins que les informations qu'elles comportent sont plus précises que celles qui figurent sur les déclarations de revenus classiques du type 2042. Aussi, la Commission a-t-elle considéré que le niveau d'agrégation minimum applicable à ces données devrait être relevé de trois à onze, au moins dans le cas d'une communication à des particuliers ou à des organismes privés. Aussi a-t-elle proposée que la règle des onze unités soit étendue à ces hypothèses lorsque les informations se rapportent à des personnes physiques, au moins dans le cas de leur communication à des particuliers ou à des organismes privés.

Enfin, le projet d'instruction imposait que, préalablement à la diffusion de données, le demandeur signe un acte par lequel il s'engage notamment à ne pas rediffuser les données en l'état à des tiers ; en revanche, les résultats des travaux effectués à partir des données pourraient eux être diffusés. De même, les demandeurs s'engagent à ne pas utiliser les informations transmises à d'autres fins que l'établissement de statistiques.

Sur ce point, la CNIL a estimé qu'au regard de la faiblesse des seuils minimum d'agrégation préconisés, il serait préférable, pour prévenir tout risque d'identification des personnes concernées par les informations statistiques, que les demandeurs s'engagent également à ne pas se livrer à une exploitation des données qui permettrait, par rapprochement avec une autre source ou toute autre méthode, d'identifier les personnes composant une catégorie agrégée.

En définitive, et après avoir fait valoir ses éléments de réflexion, la CNIL a été satisfaite de constater que l'instruction qui a été diffusée en décembre 1997 par la DGI, a repris l'ensemble de ses préconisations, notamment la doctrine en matière de seuils d'agrégation.

II. L'INTERVENTION DES COMMUNES DANS LE DOMAINE FISCAL

A. La communication aux services fiscaux d'informations relatives aux impôts locaux

Depuis la loi de finances rectificative pour 1992, les mairies peuvent communiquer aux services fiscaux des informations nécessaires au recensement des bases des impositions directes locales. Sur ce fondement, des communes ont mis en œuvre des applications informatiques visant à concrétiser cette faculté d'assistance des communes en faveur de la DGI. Toutefois, la CNIL a estimé que des communes allaient au-delà de l'objectif fixé par la loi, certaines d'entre elles ayant créé purement et simplement un service communal de contrôle fiscal (*cf.* 15e rapport, p. 203 et 16e rapport, p. 157).

En toutes occasions, la CNIL a indiqué que le contrôle des situations fiscales devait rester de la compétence exclusive de l'administration des impôts et que toute transmission de données fiscales à des tiers est interdite. De même, les renseignements communiqués aux services fiscaux ne doivent pas être le résultat de l'analyse par les services municipaux du contenu de la déclaration fiscale des assujettis.

Lors de l'examen d'un projet de création d'une base de données fiscales et foncières par la mairie d'Orléans, la Commission a constaté que le dispositif qui lui était présenté visait à mettre en oeuvre des contrôles de cohérence destinés à informer l'administration fiscale des anomalies éventuellement détectées. La Commission a par conséquent émis un avis défavorable.

Compte tenu de l'afflux des demandes d'avis émanant de collectivités locales qui souhaitent exploiter les rôles des impôts locaux, la Commission a par ailleurs décidé d'engager, en concertation avec les associations représentatives d'élus locaux, la direction générale des impôts et la direction générale des collectivités locales au ministère de l'Intérieur, une réflexion visant à définir les opérations de recensement des bases d'imposition auxquelles les communes peuvent légitimement souhaiter participer en accord avec l'administration fiscale.

Délibération n° 97-074 du 7 octobre 1997 portant avis sur trois projets d'arrêté du maire de la ville d'Orléans concernant les différentes finalités d'une base de données foncières et fiscales (Demandes d'avis n° 487 196, 487 202 et 487 211)

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 article L. 135 B, R. 135 B-1 et suivants ;

Vu l'arrêté du 16 août 1984 du ministre chargé du Budget relatif au traitement MAJIC 2 de la direction générale des impôts, modifié par un arrêté du 30 mai 1996, notamment son article 4 ;

Vu les projets d'arrêté municipal présentés par la mairie de la ville d'Orléans ;
Après avoir entendu Monsieur Thierry Cathala en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;
Considérant que le mairie d'Orléans a saisi la Commission nationale de l'informatique et des libertés de trois demandes d'avis relatives aux traitements mis en oeuvre à partir des informations conservées dans une base de données foncières et fiscales qui est constituée par la mairie à partir de différents fichiers informatisés transmis par les services de la direction générale des impôts (DGI) :

- des fichiers comportant des informations littérales cadastrales : les fichiers des voies et lieux-dits (Fantoir), des parcelles, des locaux, des propriétaires ;
- des fichiers relatifs à la fiscalité locale : les rôles généraux des taxes foncières, de la taxe d'habitation et de la taxe professionnelle ;
- un fichier comportant à la fois des renseignements cadastraux et fiscaux : le fichier nominatif taxe d'habitation.

Considérant que les trois traitements déclarés ont pour points communs d'être installés sur le même poste de travail, qui est implanté dans les locaux de la direction des affaires financières et du budget de la ville et relié à un serveur gérant plusieurs bases de données ; qu'ils sont les seuls à autoriser l'accès aux informations fiscales de la base de données foncières et fiscales ;
Considérant que les finalités de ces traitements sont :

1) pour le traitement dénommé « Observatoire fiscal », utilisé par la direction des affaires financières et du budget :
- la réalisation d'études prospectives sur l'évolution du produit global des quatre impôts directs locaux, dans le cadre de la préparation du budget de la ville ;
- l'aide au recensement des bases d'imposition directe locale, afin de communiquer à l'administration fiscale les situations jugées anormales, dans le seul cas où les opérations automatisées autorisées par la CNIL auront permis de détecter, soit des anomalies dans l'évolution du montant des impôts dus ou des éléments de leur assiette au vu du contenu des rôles généraux des impôts locaux, soit des incohérences entre les fichiers fonciers et fiscaux susmentionnés ;

2) pour l'application « Patrimoine économique », mise en oeuvre par la direction de l'action économique :
- l'analyse de la structure du tissu économique local par la production de documents de synthèse, afin d'aider à la définition de la politique de développement économique de la ville ;
- la réalisation d'analyses prospectives et rétrospectives sur l'évolution du produit de la taxe professionnelle ;
- l'évaluation de l'impact fiscal des aides municipales au développement versées aux entreprises, à partir du suivi de l'évolution des bases de taxe professionnelle des contribuables aidés par la collectivité ;
- l'aide au recensement des bases d'imposition de la taxe professionnelle, dans les conditions décrites pour le traitement « Observatoire fiscal », afin d'informer les services fiscaux des anomalies et incohérences constatées, via la direction des affaires financières et du budget ;

3) pour le traitement « Redevance spéciale des ordures ménagères », utilisé par la direction de la propreté : la détermination des usagers « professionnels » qui bénéficient d'un service rendu au titre de l'obligation d'enlèvement des ordures ménagères supérieur au montant de la taxe d'enlèvement des ordures qui est à leur charge, et pour lesquels la ville peut demander le paiement d'une redevance spéciale ;

Considérant ainsi qu'il est prévu que les anomalies et incohérences relatives aux bases d'imposition qui auront été détectées par l'administration municipale, seront transmises aux services fiscaux en vue de leur contrôle ; Considérant, à cet égard, que si l'article L. 135 B du Livre des procédures fiscales prévoit que les communes et l'administration fiscale peuvent se

communiquer mutuellement les informations nécessaires au recensement des bases des impositions directes locales, cette faculté ne saurait être mise en oeuvre dans des conditions telles que l'administration municipale exercerait des pouvoirs la faisant participer aux travaux de contrôle individuel qui relèvent de la compétence exclusive de l'administration fiscale ; Considérant, au surplus, que les projets présentés par la mairie d'Orléans recourent à un système de gestion de bases de données sans l'assortir des garanties techniques suffisantes pour prévenir tout risque découlant de la mise en œuvre d'un tel système ;
Émet, en l'état, **un avis défavorable** sur les trois projets d'arrêté municipal présentés par la mairie d'Orléans.

B. Une autre utilisation des rôles des impôts locaux par les mairies

Les collectivités locales reçoivent chaque année de l'administration fiscale les rôles des impôts locaux qui comportent les impositions émises à leur profit, et qui peuvent à leur demande leur être transmis sur support informatique. Cependant, au-delà de l'interdiction, posée par l'article L. 135 B du Livre des procédures fiscales, le risque existe que ces informations puissent être utilisées à des fins commerciales, politiques ou électorales, les conditions d'utilisation des rôles de la taxe d'habitation, de la taxe professionnelle et des taxes foncières ne sont pas précisées par les textes. Une demande d'avis de la mairie de Clermont-Ferrand, relative à l'utilisation de ces informations pour adresser aux contribuables de cette ville assujettis à la taxe d'habitation un courrier explicatif de l'augmentation de cette taxe, a donné l'occasion à la CNIL de fixer certaines limites à l'utilisation de ces fichiers pour diffuser une information auprès des contribuables locaux.

À cet égard, la Commission admet le principe que chaque collectivité puisse utiliser ces rôles pour informer les contribuables locaux des modalités de calcul des cotisations des impôts locaux, de l'évolution des conditions d'imposition et de la proportion de cet impôt parmi l'ensemble des ressources de la collectivité. Pour autant, la CNIL a précisé que l'information diffusée doit être objective et par conséquent que soit banni toute considération et tout commentaire, notamment de nature politique, ou toute évocation des incidences d'une décision prise par une autre collectivité.

Par ailleurs, la CNIL demande que l'information des contribuables s'opère sans aucune discrimination entre administrés, par exemple au regard du niveau d'imposition ; cela implique le recours aux seuls nom et adresse des contribuables pour l'envoi d'un courrier d'information. Ainsi, la Commission a manifesté son souci d'éviter toute segmentation de la population des contribuables locaux et de garantir que chaque assujetti sera, dans ce cadre, informé dans les mêmes termes sur la politique fiscale de la collectivité locale au financement de laquelle il contribue.

Enfin, la Commission recommande que les courriers indiquent clairement la provenance et l'origine des informations utilisées pour leur envoi.

Au regard de l'ensemble de ces critères, la CNIL a été conduite à émettre, en l'état, un avis défavorable au projet d'arrêté présenté par la mairie de Clermont-Ferrand.

Délibération n° 97-076 du 7 octobre 1997 portant avis sur un projet d'arrêté du maire de Clermont-Ferrand concernant l'envoi d'un courrier aux redevables de la taxe d'habitation à partir d'un fichier informatisé transmis par l'administration fiscale
(Demande d'avis n° 524 364)

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, 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 article L. 135 B, R. 135 B-1 et suivants ;

Vu le projet d'arrêté municipal présenté par la mairie de Clermont-Ferrand ; Après avoir entendu Monsieur Thierry Cathala en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Considérant que le mairie de Clermont-Ferrand 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 d'adresser à certains contribuables clermontois de la taxe d'habitation une lettre-circulaire les informant des raisons de l'augmentation, cette année, du montant global de cet impôt ; que cet envoi serait réalisé à partir du rôle général de la taxe d'habitation que la mairie a spécialement demandé à cette fin à la direction générale des impôts ;

Considérant que le Livre des procédures fiscales prévoit que les collectivités locales sont destinataires des rôles généraux des impôts directs locaux comportant les impositions émises à leur profit ; que celles-ci peuvent souhaiter que ces informations leur soient transmises sur support informatique ; qu'en outre, l'article R. 135 B-2 dudit livre prohibe toute utilisation de ces informations à des fins commerciales, politiques ou électorales ;

Considérant qu'une collectivité locale peut utiliser les rôles des impôts locaux qui lui sont transmis par l'administration fiscale pour l'information des contribuables locaux sur les modalités de calcul de la part des cotisations des impôts locaux qui lui revient, sur l'évolution des conditions d'imposition qu'elle a décidée et sur les raisons de cette évolution, ainsi que sur la part que représente cet impôt parmi l'ensemble des ressources de la collectivité ; que l'information ainsi diffusée doit cependant être objective et exclure toute autre considération ou commentaire, notamment de nature politique ;

Considérant que ces courriers doivent indiquer sans ambiguïté leur provenance et l'origine des informations utilisées pour leur envoi ; que seuls les nom et adresse des contribuables inscrits dans le fichier doivent être

exploités pour la réalisation de l'envoi, afin que l'utilisation d'un fichier administratif pour l'information de la population ne puisse pas conduire à l'envoi de messages particulièrement ciblés, adaptés et destinés à une partie seulement des contribuables d'un même impôt, afin par exemple d'aménager l'information diffusée en fonction des conditions d'imposition de ses destinataires ;

Considérant, en l'espèce, que le projet de lettre-circulaire préparé par la mairie évoque clairement les incidences, sur le niveau global de la taxe d'habitation, d'une décision prise par une autre collectivité locale et en commente les effets pour les destinataires du courrier ; qu'une telle utilisation des rôles des impôts locaux par une collectivité locale est susceptible d'être interprétée comme ayant une finalité politique, dans la mesure où elle excède le cadre d'une simple information sur les décisions qu'elle a prises elle-même et sur leurs conséquences pour les assujettis ; Considérant en outre que si doit être approuvée l'initiative d'une collectivité locale qui entend fournir aux administrés toutes les informations relatives aux modifications apportées aux impositions revenant à cette collectivité, il importe que cette information soit générale et non limitée à certaines catégories de contribuables locaux ; que dès lors le courrier ne devrait pas être adressé aux seules personnes bénéficiant d'abattements pratiqués en fonction de leur situation personnelle ;

Considérant que le projet de courrier ne mentionne pas la nature du fichier utilisé pour procéder à l'envoi ;

Considérant enfin que la finalité du traitement déclarée à la Commission ne justifie pas que les informations soient conservées au-delà de la durée des opérations d'envoi, a fortiori pendant une durée illimitée ;

Émet, en l'état, **un avis défavorable** sur le projet d'arrêté municipal présenté par la mairie de Clermont-Ferrand.

III. LE PROJET D'INTERCONNEXION DES FICHIERS FISCAUX ET SOCIAUX

Le débat sur l'échange d'informations entre les administrations grâce à l'utilisation du numéro national d'identification (NIR) renvoie aux origines de la loi du 6 janvier 1978, née de l'émotion de l'opinion publique face à un projet d'identification unique des personnes par les administrations (cf. 1er rapport, p. 7).

Ce sujet, ponctuellement relancé, avait été à nouveau d'actualité en 1996, à la suite du rapport de la mission parlementaire sur les fraudes et les pratiques abusives qui préconisait cette solution à des fins de lutte contre la fraude.

En réalité, plusieurs croisements de fichiers au sein de l'Administration, sur la base du NIR, sont déjà autorisés, le plus souvent à des fins de lutte contre la fraude, notamment sociale. Pour autant, la CNIL a toujours exigé la transparence de ces échanges à l'égard des personnes et le respect de l'article 18 de la loi du 6 janvier 1978, qui subordonne toute utilisation du répertoire national d'identification des personnes physiques, à une autorisation par décret en

Conseil d'État pris après avis de la CNIL. Cette procédure particulière se justifie par le fait que le NIR est loin d'être un numéro aléatoire, mais un numéro identifiant, les treize chiffres qui le composent revêtant une signification (sexe, mois, année, département et commune de naissance).

Dans le cadre des nouveaux pouvoirs conférés par la loi constitutionnelle n° 96-138 du 22 février 1996 au Parlement chargé de déterminer chaque année les conditions générales de l'équilibre financier de la sécurité sociale et d'en fixer les objectifs de dépenses, la CNIL avait été saisie, une première fois pour avis, du texte de deux articles du projet de loi de financement de la sécurité sociale pour 1997, prévoyant notamment la collecte du NIR par l'administration fiscale. Ce projet d'extension du NIR à la sphère fiscale, et partant l'interconnexion aisée des fichiers sociaux et des fichiers fiscaux, devait permettre aux organismes sociaux de vérifier, à partir des informations détenues par l'administration fiscale, l'exactitude ou la concordance des renseignements portés à leur connaissance par les personnes concernées. Le fait que l'administration fiscale puisse à cette occasion collecter, conserver et utiliser le NIR pour l'exercice de ses missions constituait une nouveauté et soulevait un problème de fond. La CNIL en tout cas avait estimé que l'utilisation du NIR au-delà de la sphère sociale touchait à un fondement de la loi du 6 janvier 1978, qui l'a notamment chargée de contrôler l'utilisation éventuelle d'un numéro unique d'identification des personnes. Par la suite, le Conseil d'État, consulté sur le projet de loi de financement de la sécurité sociale pour 1997, a estimé que lesdits articles devaient être disjoints du texte dans la mesure où le dispositif qu'ils instituaient était sans incidence directe et immédiate sur l'équilibre financier des régimes obligatoires de sécurité sociale (cf. 17^{e} rapport, p. 253).

En 1997, la CNIL a, une nouvelle fois, été saisie d'une disposition appelée à figurer dans un projet de loi portant diverses dispositions d'ordre économique et financier, posant le principe d'échanges automatisés d'informations entre les organismes de sécurité sociale et l'administration fiscale, et autorisant celle-ci à disposer du NIR. Cette disposition répondait essentiellement au souci de pouvoir vérifier systématiquement auprès de l'administration fiscale les ressources déclarées par les personnes qui s'adressent aux organismes sociaux pour solliciter des allocations subordonnées à condition de ressources. Ce projet n'ayant pas été adopté, notamment en raison de la dissolution de l'Assemblée nationale, la délibération qu'avait rendue le CNIL à son sujet sur le fondement de la loi du 6 janvier 1978, n'a pu recevoir d'application.

Délibération n° 97-021 du 25 mars 1997 portant avis sur un projet d'article L. 115-8 du code de la sécurité sociale

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

Vu le décret n° 82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques ;

Vu l'article R. 115-1 du code de la sécurité sociale, issu du décret n° 96-793 du 12 septembre 1996 relatif à l'autorisation d'utilisation du numéro d'inscription au répertoire d'identification des personnes physiques ;

Vu le projet d'article L. 115-8 du code de la sécurité sociale inclus dans un projet de loi comportant diverses dispositions d'ordre économique et financier, présenté par le ministère du Travail et des Affaires sociales ; Après avoir entendu Messieurs Thierry Cathala et Maurice Viennois, en leur rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Considérant que la CNIL a été saisie par le directeur de la sécurité sociale, en application de l'article 20 du décret du 17 juillet 1978, d'une disposition appelée à figurer dans un projet de loi portant diverses dispositions d'ordre économique et financier ;

Considérant que, dans les termes où il lui est soumis, ce texte a pour objet de systématiser la communication d'informations par l'administration fiscale aux organismes de sécurité sociale chargés de la gestion d'un régime obligatoire et aux institutions de retraite complémentaire obligatoire ; que ces informations concernent, selon l'exposé des motifs, la situation fiscale et les revenus des personnes ; qu'à cette fin, le texte proposé prévoit d'autoriser l'administration fiscale à collecter, conserver et utiliser le numéro d'identification au répertoire national (NIR) dans les traitements automatisés d'informations nominatives nécessaires à ces échanges ;

Considérant que ce texte vise d'une part, à simplifier les relations entre les personnes concernées et les organismes sociaux, d'autre part, à permettre à ces organismes de vérifier auprès de l'administration fiscale la concordance des éléments de ressources qui leur ont été déclarés avec ceux qui ont été portés sur les déclarations fiscales de revenus ; Considérant que seraient principalement concernés par cette disposition les retraités, les personnes sollicitant une allocation subordonnée à condition de ressources ainsi que les travailleurs indépendants ; Considérant que, s'agissant des retraités, l'exonération de la cotisation d'assurance maladie et des contributions sociales (CSG, CRDS) est liée à la situation fiscale des bénéficiaires au regard de l'impôt sur le revenu et de la taxe d'habitation ; que dès lors, les personnes concernées doivent actuellement adresser un avis d'imposition ou de non-imposition aux organismes débiteurs des avantages de retraite et informer ces organismes lorsqu'un changement significatif intervient dans leur situation fiscale ; que le ministère des Affaires sociales fait valoir que la majorité des personnes concernées relève de plusieurs régimes de retraite et est, en conséquence, assujettie à des obligations déclaratives répétées, d'autant plus difficiles à comprendre que la législation est complexe ; que ces formalités ne sont parfois pas accomplies, par ignorance ou lassitude, alors même que dans une proportion importante les changements de situation contributive pourraient bénéficier aux personnes concernées ; que le principe d'un échange automatisé d'informations entre les organismes sociaux et l'administration

fiscale permettrait d'éviter aux retraités d'avoir à accomplir de telles démarches ;

Considérant que, s'agissant des personnes sollicitant ou percevant une allocation subordonnée à condition de ressources, le projet vise à permettre aux organismes payeurs d'opérer une comparaison systématique des déclarations de ressources souscrites par les allocataires auprès d'eux avec la déclaration fiscale de revenus ; que de nombreuses allocations sont subordonnées à condition de ressources parmi lesquelles les plus importantes sont les aides au logement (6 millions de bénéficiaires en 1995), le revenu minimum d'insertion (946 000 bénéficiaires) l'allocation adulte handicapé (plus de 600 000 bénéficiaires), l'allocation parent isolé (170 000 bénéficiaires) ;

Considérant que, s'agissant des travailleurs non salariés des professions non agricoles, dont les cotisations sociales sont assises sur les revenus qu'ils déclarent à leur organisme de sécurité sociale, les ressortissants de ce régime doivent transmettre à leur caisse de sécurité sociale une déclaration de revenus qui permet à la fois de calculer les cotisations sociales (assurance maladie, allocations familiales, assurance vieillesse) après avoir recherché, lorsque l'intéressé exerce plusieurs activités professionnelles, son activité principale ;

Considérant que le projet de texte complète ce dispositif d'échanges en prévoyant que l'administration fiscale, qui ne dispose pas à l'heure actuelle du NIR dans ses propres fichiers, serait désormais autorisée à collecter, enregistrer et utiliser cet identifiant dans le cadre de ces échanges ;

Considérant que le ministère des Affaires sociales, comme les organismes concernés, fait valoir que les échanges informatisés qui sont à l'heure actuelle opérés sur la base des éléments d'état civil (nom, prénoms, date et lieu de naissance) et sur l'adresse des personnes concernées seraient insatisfaisants ; que dans une fourchette de 30 % à 40 % des cas, l'administration fiscale se trouverait dans l'impossibilité de restituer aux organismes sociaux qui en font la demande les éléments de comparaison sollicités ; qu'à cet égard, le recours à un identifiant commun aux fichiers appelés à être rapprochés pourrait conférer à ces échanges un caractère exhaustif qui permettrait de déterminer de façon plus fiable le montant des prélèvements à opérer sur les pensions de retraite ainsi que de mieux contrôler les conditions d'octroi de prestations soumises à condition de ressources et les modalités de calcul des cotisations sociales des travailleurs indépendants ; que l'identifiant commun proposé, en raison du caractère efficace et peu coûteux que représenterait cette solution selon le ministère des Affaires sociales, serait le NIR ;

Considérant que l'une des motivations de l'adoption de la loi du 6 janvier 1978 a été d'éviter qu'une personne puisse être identifiée par un même numéro commun à diverses administrations (le numéro d'inscription au répertoire national d'identification des personnes physiques, plus communément appelé numéro de sécurité sociale) ; que les identifiants nationaux comme les interconnexions de fichiers publics font l'objet, dans la plupart des démocraties dotées d'une législation des données à caractère personnel, d'une protection particulière ;

Considérant que la Commission doit se prononcer à la lumière du principe posé par l'article 1er de la loi du 6 janvier 1978 selon lequel « l'informati-

que 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 » et des précautions particulières dont le législateur a entendu entourer l'utilisation du numéro de sécurité sociale et tout particulièrement dans le cas des interconnexions de fichiers publics ;

Considérant cependant que ces précautions n'ont pas eu pour objet et ne doivent pas avoir pour effet de protéger les fraudeurs ; qu'à cet égard, la Commission nationale de l'informatique et des libertés rappelle, comme le Conseil constitutionnel l'a souligné dans sa décision 83-164 du 29 décembre 1983 « que l'exercice des libertés et droits individuels ne saurait en rien excuser la fraude fiscale ni en entraver la légitime répression » ; que s'agissant de fonds publics, ce principe doit également s'appliquer à la fraude aux prestations sociales ;

Considérant d'ailleurs que la CNIL a donné des avis favorables à diverses expérimentations ou rapprochements informatisés de fichiers sociaux avec des fichiers fiscaux ; que tel est notamment le cas pour les fichiers des caisses d'assurance vieillesse et des caisses d'allocations familiales ; qu'eu égard respectivement aux montants des prélèvements et/ou des versements indus, constatés en particulier dans les premiers bilans issus de ces rapprochements ainsi que dans le rapport de la mission parlementaire sur les fraudes et pratiques abusives, la fraude estimée aux prestations sociales visées par ce projet, toutes prestations confondues, serait nettement inférieure à la fraude estimée de l'impôt sur les sociétés ou à celle de l'impôt sur le revenu ;

Considérant que s'il incombe aux pouvoirs publics de déterminer les priorités de lutte contre la fraude et les moyens à mettre en œuvre pour y parvenir, il entre dans les missions de la CNIL d'appeler l'attention du législateur, à l'heure des choix qu'il lui revient de faire, sur les effets de l'utilisation de l'informatique sur le fonctionnement des institutions démocratiques ;

Considérant que l'objectif du projet, tel qu'il résulte du premier alinéa du texte proposé, en ce qu'il pose le principe du contrôle par les organismes sociaux des déclarations de ressources qui leur sont faites par rapprochement des informations qu'ils détiennent avec celles de l'administration fiscale, est légitime au regard des principes ci-dessus rappelés ; qu'en outre, le souci de simplification des démarches administratives devrait conduire à substituer aux multiples déclarations sociales ou fiscales, une déclaration unique, à charge pour l'organisme qui en serait destinataire de ventiler les informations pertinentes à chacun des organismes ou administrations concernés ; que sans cette nécessaire contrepartie, le projet de texte pourrait être interprété comme visant à organiser des contrôles systématiques sur les personnes les plus démunies ;

Mais considérant que l'autorisation pour l'administration fiscale de collecter, enregistrer et utiliser le NIR dans le cadre des échanges projetés aurait pour effet d'étendre l'usage de cet identifiant commun à une nouvelle administration ; qu'outre l'ensemble des organismes de sécurité sociale, l'ANPE, l'UNEDIC et les ASSEDIC ainsi que les employeurs collectent et enregistrent le NIR dans leurs fichiers ; que, plus récemment, les professionnels de santé ont été autorisés à utiliser cet identifiant qui est désormais associé à des données médicales, ces dernières devant d'ailleurs, par le codage des pathologies, être plus précisément enregistrées dans les fichiers des caisses d'assurance maladie ;

Considérant que le principe de proportionnalité et la crainte de l'irréversibilité de l'organisation informatique qui résulterait de l'adoption de la disposition proposée inspirent de sérieuses réserves sur le choix du NIR comme élément de rapprochement des fichiers fiscaux et sociaux ; Considérant en effet que si la mention du NIR dans un fichier n'autorise pas, à elle seule, des transferts d'informations entre les administrations qui en disposent, de tels transferts étant d'ailleurs pénalement sanctionnés s'ils ne trouvent pas leur fondement dans une disposition légale ou s'ils aboutissent à la violation de secrets légalement protégés, la généralisation d'un identifiant commun à des organismes de nature très différente fait courir le risque qu'en des périodes dans lesquelles les principes démocratiques ne seraient plus respectés ou garantis, un même critère d'interrogation des fichiers administratifs pourrait, sur cette seule information, les révéler toutes ; Considérant en outre, que si cette extension du NIR aux fichiers fiscaux n'a pas pour objet de permettre à l'administration concernée d'utiliser cet identifiant à des fins fiscales, le fait même de son intégration dans ces fichiers pourrait conduire, malgré les précautions prises, à une extension de son utilisation à des fins fiscales, voire même, par capillarité, à son recueil par d'autres organismes et administrations, ce qui conduirait à faire du NIR l'identifiant national unique ;

Or, considérant que le taux d'échec des rapprochements qui sont actuellement opérés en l'absence d'identifiant commun entre la sphère fiscale et la sphère sociale pourrait, selon les informations dont dispose la Commission, considérablement diminuer si les organismes sociaux interrogeaient l'administration fiscale sur la base de données d'état civil complètes et préalablement certifiées par l'INSEE, ce qui, à l'heure actuelle n'est pas toujours le cas ; Considérant en outre, que l'utilisation d'un autre identifiant que le NIR pourrait être aussi efficace dès lors que cet identifiant serait individuel, stable et pourrait être certifié par l'INSEE ; que le numéro SPI dont est dotée l'administration fiscale présente ces caractéristiques et pourrait dès lors, s'il était systématiquement transmis aux organismes sociaux, éviter de recourir au NIR ; que cette solution présenterait l'avantage de cantonner l'usage d'un identifiant commun non signifiant aux relations socio-fiscales ; Considérant enfin qu'une autre solution, préconisée par M. de la Martinière dans un rapport remis au Premier ministre en 1995, consisterait à confier à un organisme tiers la gestion d'une table de concordance entre les identifiants respectifs des organismes sociaux et de l'administration fiscale ; Considérant dès lors qu'une réflexion plus approfondie sur les solutions propres à atteindre l'objectif que le ministère des Affaires sociales s'est assigné devrait être conduite avant que soit arrêté un choix définitif ; **Émet les réserves** ci-dessus exprimées sur le deuxième alinéa de la disposition qui lui a été soumise.

Chapitre 3

JEUNESSE, ÉDUCATION

ET SPORTS

I. L'INSCRIPTION TELEMATIQUE À L'UNIVERSITÉ

Dans un souci de simplification des procédures, de nombreuses universités mettent en œuvre des services télématiques de gestion des inscriptions. La CNIL a toujours manifesté beaucoup de vigilance à leur sujet, afin notamment de préserver le principe d'égalité entre les étudiants. Aussi, a-t-elle précisé que le recours au minitel ne devait permettre que d'organiser les rendez-vous pour les inscriptions définitives. Par ailleurs, la Commission a recommandé qu'une page-écran apparaisse dès l'ouverture du service pour informer les personnes concernées de l'existence du traitement, dans les conditions prévues par l'article 27 de la loi « Informatique et Libertés » (cf. 10^{e} rapport, p. 137).

Un arrêt du Conseil d'État du 15 janvier 1997 a renforcé l'encadrement de l'usage du minitel pour les inscriptions à l'université. En l'espèce, le Conseil s'est prononcé sur l'inscription par minitel dans la filière « sections d'activités physiques et sportives » de l'université de Rennes II, filière dont la capacité d'accueil est très nettement insuffisante au regard des demandes d'inscription présentées.

La procédure, contestée par des étudiants dont les demandes d'inscription n'avaient pas abouti, consistait à retenir, dans l'ordre chronologique des connexions effectuées, les confirmations de demande d'inscription reçues sur minitel. Tous les candidats avaient été informés de la date et de l'heure précises du démarrage des opérations d'inscription.

Le Conseil d'État a déclaré illégale cette procédure dans la mesure où elle « méconnaît le principe de l'égalité de traitement entre les candidats eu égard aux conditions d'équipement télématique et informatique des intéressés, aux possibilités techniques de connexion et aux différences qui en résultent dans les conditions d'acheminement de leurs appels vers le serveur télématique de l'université ».

II. LA MODIFICATION DU TRAITEMENT « SCOLARITÉ

La CNIL a donné un avis favorable à la modification du traitement « SCOLARITÉ » de gestion administrative et pédagogique des élèves de l'enseignement public du second degré ; ce traitement avait reçu un avis favorable par délibération n° 93-074 du 7 septembre 1993 *(cf.* 14e rapport, p. 119).

En effet, le ministère de l'Éducation nationale, de la Recherche et de la Technologie a souhaité que tous les établissements publics d'enseignement du second degré puissent transmettre, sur support magnétique, aux caisses d'allocations familiales, des certificats de scolarité concernant leurs élèves ; l'objectif étant d'accélérer le paiement de l'allocation de rentrée scolaire versée aux élèves âgés de 16 à 18 ans sur présentation d'un certificat de scolarité.

L'expérimentation de cette procédure, qui présente l'avantage d'éviter toute démarche aux familles et aux établissements scolaires, s'étant révélée très positive, la Caisse nationale d'allocations familiales (CNAF) et le ministère de l'Éducation nationale ont souhaité sa généralisation.

Ainsi, chaque établissement devra transmettre à la CAF, des données concernant l'ensemble des élèves inscrits pour la rentrée, précisant l'identité et la date de naissance de l'élève, l'identité de l'un des parents et la commune de résidence. La CAF identifiera ensuite les enfants bénéficiaires et enregistrera qu'un certificat de scolarité a été reçu. Les données visant les élèves qui ne sont pas concernés par le versement de l'allocation seront détruites.

Délibération n° 97-059 du 8 juillet 1997 portant avis sur la déclaration de modification du traitement « SCOLARITÉ », présentée par le ministère de l'Éducation nationale, de la Recherche et de la Technologie

(Demande d'avis n° 309 970)

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 ;

Vu le décret n° 78-774 modifié du 17 juillet 1978 portant application de la loi du 6 janvier 1978 ;

Vu l'article R. 543-4 du code de la sécurité sociale relatif à l'allocation de rentrée scolaire ;

Vu la délibération n° 93-074 du 7 septembre 1993 de la CNIL portant avis sur la mise en œuvre, par le ministère de l'Éducation nationale, du traitement « SCOLARITÉ » ;

Vu le projet d'arrêté présenté par le ministre de l'Éducation nationale, de la Recherche et de la Technologie ;

Après avoir entendu Monsieur Michel Bernard, 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 la direction des lycées et collèges du ministère de l'Éducation nationale, de la Recherche et de la Technologie, d'une modification du traitement automatisé d'informations nominatives dénommé « SCOLARITÉ » ; Considérant que le traitement « SCOLARITÉ » a pour objet d'assurer la gestion administrative, pédagogique et financière des élèves par les établissements publics d'enseignement de second degré, la gestion académique et l'établissement de statistiques par les rectorats et les directions départementales des services de l'Éducation nationale, de la Recherche et de la Technologie, la gestion prévisionnelle et la mise en oeuvre d'études statistiques par l'administration centrale ; que le système est articulé autour de trois bases de données : la base élèves au niveau de l'établissement scolaire (BEE), la base élèves au niveau académique (BEA), la base centrale de pilotage (BCP) au niveau de l'administration centrale ; Considérant que la modification soumise à l'avis de la Commission a pour objet d'autoriser les établissements publics d'enseignement du second degré à transmettre, sur support magnétique dès le mois de juillet, à la caisse d'allocations familiales concernée, des certificats de scolarité concernant les élèves inscrits pour la rentrée de septembre ;

Considérant que les données transmises seront relatives au : nom, prénom, date de naissance de l'élève, nom et prénom de l'un des parents, commune de résidence ;

Considérant que chaque caisse d'allocations familiales, après qu'elle aura identifié les bénéficiaires de l'allocation de rentrée scolaire, procédera à la destruction des données relatives aux élèves qui ne sont pas concernés par cette allocation ;

Considérant que l'intérêt de cette procédure est de faciliter et d'accélérer le paiement de l'allocation de rentrée scolaire versée par la caisse d'allocations familiales aux élèves âgés de 16 à 18 ans ; qu'elle présente l'avantage d'éviter toute démarche aux parents ; qu'elle a fait l'objet d'une expérimentation en juillet 1996 qui a donné des résultats satisfaisants. Considérant qu'il y a lieu de préciser la rédaction de l'article 1 du projet d'arrêté en ce qui concerne la nature des données transmises ;

Émet un avis favorable au, projet d'arrêté portant modification de l'arrêté initial créant « SCOLARITÉ » sous réserve que l'article 1er soit rédigé

de la manière suivante : « En vue du règlement de l'allocation de rentrée scolaire pour les élèves âgés de 16 à 18 ans, les caisses d'allocations familiales sont destinataires des données suivantes : nom, prénom, date de naissance de l'élève, nom et prénom de l'un des parents, commune de résidence ».

III. L'EXPERIMENTATION DU TRAITEMENT « CARTÉCOLE »

En 1995, la mairie de Paris a mis en œuvre un projet de rénovation du système de gestion des effectifs, des paiements et des inscriptions scolaires. Dans cette perspective, la direction des affaires scolaires (DASCO) a implanté, à titre expérimental, un traitement dénommé « CARTÉCOLE » dans quatre établissements du XIII^{e} arrondissement de Paris (deux maternelles et deux écoles élémentaires).

Cette expérimentation a consisté à tester :
- l'utilisation d'une carte à puce par les enfants comme moyen d'identification et de paiement de la restauration, des centres de loisirs, des études surveillées et des garderies ;
- l'organisation du système et sa fonction de sous-régie au niveau de l'école.

En pratique, l'intégration au dispositif « CARTÉCOLE » nécessite le recueil de l'identité de l'enfant et de ses responsables légaux, la connaissance des services qu'il fréquente et, le cas échéant, d'un régime alimentaire. Une carte à puce est alors délivrée gratuitement à chaque enfant inscrit à l'école. Le matin, l'enfant introduit sa carte dans une borne reliée à un micro-ordinateur dans i'école et sélectionne les services dont il a besoin ; le compte alimenté par les parents est débité lors de chaque utilisation de la carte. Ce système présente l'intérêt essentiel d'étaler les paiements et de ne régler que ce qui est effectivement consommé.

Si l'accueil réservé à ce système par les parents a été plutôt favorable au début de sa mise en œuvre, sa systématisation et son extension à une finalité d'appel automatique des enfants ont en revanche été assez mal ressenties, même par certains directeurs d'écoles. Face à ces craintes et critiques, la DASCO a d'ailleurs conclu qu'il convenait de ne pas imposer le système.

En 1997, la DASCO a saisi la CNIL d'une déclaration de modification du traitement « CARTÉCOLE » visant à étendre son expérimentation à cinq autres écoles et à intégrer la gestion de la restauration du personnel de l'établissement, également doté d'une carte à puce.

À cette occasion, la CNIL a rencontré les représentants de la DASCO pour tirer les enseignements d'une année d'expérimentation. La Commission a par ailleurs effectué une visite sur place. À l'issue de ces démarches, la CNIL a rendu un avis favorable à la poursuite de l'expérimentation dans les nouvelles conditions présentées par la DASCO.

Délibération n° 97-033 du 6 mai 1997 portant avis sur la déclaration de modification du traitement « CARTÉCOLE », présentée par la mairie de Paris

(Demande d'avis n° 391 900)

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 ;

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 maire de Paris du 1er décembre 1995 portant création du traitement automatisé d'informations nominatives dénommé « CARTÉCOLE » ;

Vu le projet d'arrêté portant modification de l'arrêté du maire de Paris du 1er décembre 1995 ;

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

Considérant que la Commission nationale de l'informatique et des libertés est saisie, par la direction des affaires scolaires de la mairie de Paris, d'une déclaration de modification du traitement automatisé d'informations nominatives dénommé CARTÉCOLE, dont la finalité principale est la gestion des effectifs scolaires du premier degré, de la restauration et des activités périscolaires ;

Considérant que ce traitement fait l'objet, depuis novembre 1995, d'une expérimentation dans quatre écoles du XIIIe arrondissement de Paris ; que cette expérimentation vise à tester l'utilisation d'une carte à puce par chaque enfant comme moyen d'identification et de paiement de la restauration, des centres de loisirs, des études surveillées et des garderies ;

Considérant que la modification envisagée par la direction des affaires scolaires a pour but d'étendre cette expérimentation à quatre autres écoles situées dans le XIIIe arrondissement ainsi

qu'à une école du XVIIIe arrondissement ; qu'elle vise à gérer également la restauration des personnels des établissements concernés ;

Considérant que les parents concernés peuvent refuser l'utilisation de la carte par leurs enfants ; qu'ils sont clairement informés des modalités de fonctionnement dudit système ;

Émet un avis favorable au projet d'arrêté portant modification du traitement.

Demande à être informée du bilan de cette nouvelle phase d'expérimentation.

IV. LES DONNEES DETENUES PAR LES FÉDÉRATIONS SPORTIVES

Saisie par la société Bayard-Presse d'une demande de cession des coordonnées de 15 000 jeunes licenciés âgés de 6 à 9 ans, la fédération française de karaté a souhaité obtenir de la CNIL des précisions concernant les modalités d'information des personnes visées par ces cessions.

En réponse, la CNIL a indiqué aux représentants de la fédération que les responsables légaux des licenciés mineurs devaient impérativement être informés que les coordonnées de leurs enfants étaient susceptibles d'être cédées à une société extérieure et utilisées à des fins de prospection commerciale et avisés de leur droit de s'y opposer.

Il a été précisé que la solution envisagée par la fédération, qui consistait à adresser une lettre circulaire aux clubs, destinée à l'affichage, n'était pas suffisante au regard des exigences de protection des données.

Aussi, la CNIL a-t-elle recommandé que cette information soit individualisée par le biais, par exemple, d'une mention figurant sur la fiche d'adhésion à la fédération, accompagnée le cas échéant d'une case à cocher destinée aux parents qui ne souhaitent pas que leurs enfants deviennent une cible de prospection commerciale à raison de l'exercice de ce sport.

Par la suite, la fédération a indiqué à la CNIL qu'elle suivrait ses préconisations, notamment en indiquant sur chaque licence, document personnel et signé, les prescriptions de la loi du 6 janvier 1978 concernant le droit d'accès et de rectification, ainsi que la possibilité de s'opposer à la cession des données.

Chapitre 4

JUSTICE

I. LES CONTROLES D'ACCES DANS LES ÉTABLISSEMENTS PÉNITENTIAIRES

A. Le contrôle des familles des détenus

Le code de procédure pénale permet aux détenus de recevoir la visite des membres de leur famille ou de toute autre personne, sous réserve du maintien de la sécurité et du bon ordre dans l'établissement pénitentiaire. Ces visites se déroulent obligatoirement dans le parloir de l'établissement. Les permis de visite sont délivrés par le magistrat instructeur pour les prévenus et par le chef de l'établissement pour les condamnés. Ces permis peuvent être permanents ou valables uniquement pour un nombre limité de visites.

Le ministère de la Justice a souhaité instituer une procédure automatisée de gestion de ces visites (prises de rendez-vous, organisation des parloirs, délivrance des permis de visites et organisation des déplacements des détenus au sein des établissements pénitentiaires). L'application se limite aux seules visites des familles des détenus, et le projet de collecter la profession des visiteurs ayant, en définitive, été abandonnée les catégories d'informations nominatives visées par le traitement concernent les détenus (identité, date de naissance, numéro d'écrou, catégorie pénale du détenu, autorité qui instruit son dossier, quartier d'affectation, numéro de cellule, numéro du permis de visite) et les visiteurs (identité, degré de parenté, date et lieu de naissance, numéro de pièce d'identité, adresse, type et numéro du permis de visite, nombre d'autorisations de visite si le permis n'est pas délivré à titre permanent, autorité qui a délivré le permis de visite, jours et horaires autorisés). Enfin, la durée de conservation des informations collectées a été affinée afin d'éviter la constitution de véritables

historiques des visites ; ainsi, les informations relatives aux visites sont automatiquement effacées dès qu'elles ont eu lieu, tandis que celles se rapportant aux titulaires du permis de visite sont conservées pendant la durée de validité du permis de visite. Toutefois, le défaut d'utilisation d'un permis de visite pendant une période de deux ans, soit à compter de sa délivrance, soit à compter de la dernière visite, entraîne l'effacement automatique des informations relatives à l'identité de son titulaire. Dans ces conditions, la CNIL a émis un avis favorable au projet d'arrêté portant création d'un modèle type concernant ce traitement.

Délibération n° 97-004 du 21 janvier 1997 relative à la demande d'avis du ministère de la Justice portant création d'un modèle type de traitement ayant pour objet la gestion des visites en établissement pénitentiaire des ramilles des détenus (Demande d'avis n° 451 142)

La Commission nationale de l'informatique et des libertés ;

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

Vu le code de procédure pénale, notamment ses articles D. 64, D. 403 et D. 404 ;

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

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

Vu le projet d'arrêté du garde des Sceaux, ministre de la Justice ;

Après avoir entendu Monsieur Christian Dupuy, 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 a été saisie par le ministère de la Justice d'une demande d'avis relative à la création d'un modèle-type de traitement, appelé à être mis en oeuvre dans les établissements pénitentiaires, destiné à assurer la gestion des visites en établissement pénitentiaire des familles des détenus ; Considérant qu'en application de l'article D. 404 du code de procédure pénale, les détenus sont autorisés à recevoir la visite des membres de leur famille ;

Considérant qu'en application de l'article D. 403 du code de procédure pénale, les permis de visite sont délivrés par le magistrat instructeur pour les prévenus et par le chef de l'établissement pour les condamnés ; que ces permis peuvent être permanents ou valables uniquement pour un nombre limité de visites ;

Considérant que les informations nominatives collectées sont, s'agissant des détenus, les nom et prénom, la date de naissance, le numéro d'écrou, la catégorie pénale, l'autorité qui instruit le dossier, le quartier d'affectation et le numéro de cellule, ainsi que le numéro du permis de visite et, s'agissant des visiteurs, les nom et prénom, leur degré de parenté avec le détenu, les date et lieu de naissance, le numéro de leur carte d'identité ou de leur

passeport, l'adresse, le type et le numéro du permis de visite, le nombre d'autorisations de visite si le permis n'est pas délivré à titre permanent, l'autorité qui a délivré le permis de visite, les conditions de visite, les jours et horaires de visite, ainsi que le type de parloir ;

Considérant que ces informations sont pertinentes au regard de la finalité assignée au traitement ;

Considérant que les destinataires des informations traitées sont, chacun en ce qui le concerne, les magistrats et les chefs d'établissement pénitentiaire, qui délivrent les permis de visite, et les agents de l'administration pénitentiaire de fonction au service de la détention et au service des visites de l'établissement concerné ;

Considérant que les informations relatives à l'identité des visiteurs sont conservées durant la période de validité du permis dont ils bénéficient ; que ces informations sont effacées dès la levée d'écrou du détenu si elle intervient avant l'expiration du permis de visite ou à l'issue d'un délai de deux années à compter de sa date de délivrance ou de la dernière visite en cas d'inutilisation du permis de visite par son bénéficiaire ;
Considérant que les informations relatives aux visites sont automatiquement effacées dès qu'elles ont eu lieu ou dès que le créneau de temps qui leur était alloué est expiré ; qu'en pratique, cet effacement interviendra, au plus tard, dans un délai d'un mois à compter de la visite ;

Considérant que le droit d'accès des personnes physiques aux informations nominatives les concernant s'exerce auprès du chef d'établissement pénitentiaire ;
Considérant que les intéressés en sont informés, s'agissant des détenus, par un affichage dans les couloirs d'accès aux cours de promenade et, s'agissant des visiteurs, par un affichage dans le local réservé à leur accueil ; Considérant qu'en application du second alinéa de l'article 26 de la loi du 6 janvier 1978, le projet d'acte réglementaire exclut la possibilité pour une personne de se prévaloir, à l'égard de ce traitement, de la faculté d'opposition énoncée par l'alinéa premier de cet article ;

Considérant que les directeurs d'établissement pénitentiaire qui souhaiteront mettre en œuvre un tel traitement procéderont au moyen d'une déclaration de conformité adressée à la Commission nationale de l'informatique et des libertés ;

Considérant qu'un descriptif des mesures de sécurité et de confidentialité entourant le traitement devra être joint en annexe ;
Émet un avis favorable au projet d'arrêté du garde des Sceaux, ministre de la Justice, portant création d'un modèle-type de traitement destiné à assurer la gestion des visites en établissement pénitentiaire des familles des détenus.

B. Le contrôle du personnel pénitentiaire et des intervenants professionnels extérieurs

La direction de l'administration pénitentiaire a souhaité implanter un système de contrôle par badges des accès aux établissements pénitentiaires. Ce dispositif est destiné à remplacer le registre de toutes les personnes entrantes et sortantes prévu par l'article D. 279 du code de procédure pénale, et sur lequel doivent être également inscrits l'heure et le motif de l'entrée ou de la sortie. Le

traitement qui en résulte vise donc tous les intervenants professionnels extérieurs (magistrats, avocats, enseignants, visiteurs de prisons, personnels médicaux, aumôniers...) et tout le personnel pénitentiaire.

Concrètement, une carte à puce comportant la photographie du professionnel, ses noms et prénoms, la durée de validité de l'autorisation d'accès ainsi que les lieux d'accès autorisés pour son détenteur, doit être insérée dans une des consoles de lecture situées à la porte principale et à la grille de détention. À cette occasion, le traitement enregistre des informations qui varient en fonction du régime d'accès des personnes qui se présentent, c'est-à-dire selon qu'il s'agit de personnel pénitentiaire, d'intervenants professionnels (assistantes sociales...) ou encore de visiteurs extérieurs (médecins...).

La CNIL a demandé que l'information des personnes concernant ce traitement soit améliorée ; aussi, outre l'affichage dans les locaux de l'établissement pénitentiaire d'une note destinée aux visiteurs et aux personnels, la direction de l'administration pénitentiaire a précisé que celle-ci serait remise à chaque personne lors de la délivrance du badge d'accès et comporterait les mentions des articles 27, 34 et 36 de la loi du 6 janvier 1978.

Un avis favorable a été donné à ce modèle de traitement auquel chaque établissement devra se conformer ; les mesures de sécurité adoptées pour garantir la confidentialité des données et les dispositions prises pour assurer l'information des personnels et des visiteurs concernés devront être précisées au cas par cas.

Délibération n° 97-036 du 27 mai 1997 portant avis sur le modèle type de traitement présenté par le ministère de la Justice concernant la gestion des contrôles d'accès des personnels dans les établissements pénitentiaires

(Demande d'avis n° 451 139)

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 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu les articles D. 196, D. 278 et D. 279 du code de procédure pénale ; Vu le projet d'arrêté présenté par le ministère de la Justice ; Après avoir entendu Monsieur Hubert Bouchet 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 de traitement, appelé à être mis en oeuvre dans les établissements pénitentiaires et destiné à assurer le contrôle des accès des personnels pénitentiaires et des intervenants professionnels ou bénévoles dans ces établissements ; que ce traitement ne s'applique ni aux détenus, ni à leur famille ;

Considérant que le traitement automatisé trouve son fondement dans l'article D. 279 du code de procédure pénale disposant qu'un registre de toutes les personnes entrant ou sortant de l'établissement pénitentiaire doit être tenu ;

Considérant que les informations nominatives enregistrées sont : les photographies, les noms, prénoms, date de naissance, l'accès en détention, l'accompagnement en détention, les entrées et sorties de la zone de détention et l'autorité qui a autorisé l'accès ;

Considérant que ces informations sont pertinentes au regard de la finalité poursuivie ;

Considérant que les destinataires des informations sont le service de l'établissement chargé de l'établissement des cartes et le directeur de l'établissement pénitentiaire ;

Considérant que les informations relatives à l'identité des cartes d'accès sont conservées le temps de la validité de cet accès ; qu'en ce qui concerne les personnes appelées à accéder aux établissements de façon permanente, ces informations sont renouvelées chaque premier janvier ;

Considérant que les données relatives aux mouvements des personnes sont conservées pendant un an afin de posséder une antériorité de recherche suffisante en cas d'enquête relative à la sécurité de l'établissement ;

Considérant que des mesures des flux de circulation interne des établissements seront effectuées, afin de connaître le nombre de personnes entrant et sortant de l'établissement et de la zone de détention ;

Considérant que le droit d'accès prévu par l'article 34 de la loi du 6 janvier 1978 s'exercera auprès des directeurs des établissements pénitentiaires ; que l'information relative à ce droit d'accès sera effectuée par la remise d'une note aux personnels et visiteurs concernés, lors de la délivrance du badge ;

Considérant qu'en application du second alinéa de l'article 26 de la loi du 6 janvier 1978, le projet d'acte réglementaire exclut la possibilité pour une personne de se prévaloir, à l'égard de ce traitement, de la faculté d'opposition énoncée par l'alinéa premier de cet article ;

Considérant que les directeurs d'établissement pénitentiaire qui souhaiteront mettre en oeuvre un tel traitement adresseront une déclaration de conformité à la Commission nationale de l'informatique et des libertés accompagnée d'une annexe sur les sécurités mises en oeuvres ;

Émet un avis favorable au projet d'arrêté du garde des Sceaux, ministre de la Justice, portant création d'un modèle type de traitement relatif à la gestion des accès des personnels aux établissements pénitentiaires.

II. LA GESTION DE LA POPULATION PENALE

Aux termes de la loi du 22 juin 1987 qui définit les missions du service public pénitentiaire, il est prévu que l'administration pénitentiaire participe à l'exécution des décisions et sentences pénales et au maintien de la sécurité publique, favorise la réinsertion sociale des personnes et assure l'individualisation des peines.

Dans ce contexte, la direction de l'administration pénitentiaire a élaboré un système de gestion centralisée de la population pénale qui vise à améliorer les conditions d'affectation et de prise en charge des détenus et à faciliter les transferts d'un établissement à un autre.

Par nature, cette application a vocation à recueillir de nombreuses informations relatives aux détenus et aux modalités d'incarcération, auxquelles s'ajoutent éventuellement des informations concernant l'appartenance à un mouvement terroriste ou une organisation criminelle. Le ministère de la Justice entend ainsi rationaliser l'affectation des détenus au regard de la sécurité des établissements pénitentiaires. Cette information étant de nature à faire apparaître indirectement les opinions politiques, philosophiques ou religieuses, la Commission a été saisie d'un projet de décret portant application à ce traitement des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978, projet qui, compte tenu de l'intérêt public qui s'attache en l'espèce à la connaissance des informations, a recueilli un avis conforme de la CNIL.

Par ailleurs, l'application identifie les détenus qui doivent être particulièrement surveillés, c'est-à-dire les détenus :
- inscrits au fichier tenu par l'office central de répression du grand banditisme ou en relation avec une personne figurant dans ce fichier ;
- relevant de mesures spéciales de sécurité en raison des risques importants qu'ils présentent pour l'ordre public ;
- incarcérés dans un établissement de sécurité renforcée ou dans les locaux de plus grande sécurité ;
- apparaissant dangereux par leur comportement en détention, notamment parce qu'ils ont commis ou risquent de commettre des agressions ou des évasions.

La mise en œuvre de ce traitement informatique a été confiée au bureau de l'individualisation et des régimes de détention, qui est notamment chargé de définir les régimes de détention et les règles relatives à la répartition des condamnés entre les différents établissements pénitentiaires, et d'organiser des transferts des détenus au niveau national et international ; enfin, il est à souligner que ce bureau donne aux directeurs régionaux et aux chefs d'établissement les instructions nécessaires au traitement des incidents individuels et collectifs impliquant des détenus et traite les requêtes des prisonniers.

Les informations sont effacées cinq années après la date de libération, à l'exception des informations relatives à l'identité des personnes (nom, prénom, date de naissance, sexe, alias éventuels et nationalité), qui sont effacées dix années après la libération, cette durée étant justifiée, selon le ministère, par le risque de récidives.

La CNIL a estimé que ce long délai de conservation devait être apprécié au regard, d'une part de l'engagement de l'administration pénitentiaire d'apurer annuellement son fichier et d'autre part, de la stricte interdiction qu'il soit interconnecté. Aussi, la CNIL a-t-elle donné un avis favorable au projet d'arrêté portant création de ce traitement sous réserve qu'il soit obligatoirement rendu

compte chaque année à la CNIL des opérations de vérification, de mise à jour et d'apurement du fichier.

Dans le même temps, la CNIL a donné un avis favorable à un autre projet de gestion informatique de la population pénale, comparable dans sa philosophie à l'application centrale, mais appelé à être mis en œuvre au sein des directions régionales des services pénitentiaires. Toutefois, il convient de noter que l'éventuelle appartenance des intéressés à un réseau de délinquance organisée ne figure pas parmi les informations collectées au niveau régional, marquant ainsi le caractère plus administratif de cette application. Quoi qu'il en soit, la Commission a demandé que le projet d'arrêté portant création de ce traitement précise clairement, à l'instar de l'application centrale, que s'agissant d'un fichier qui intéresse la sûreté de l'État et la sécurité publique, le droit d'accès aux informations s'exerce par l'intermédiaire d'un membre de la CNIL, magistrat ou ancien magistrat. De même, la Commission a souhaité que les directions régionales qui souhaiteront mettre en oeuvre cette application complètent la déclaration de conformité à ce modèle type, d'un descriptif des mesures de sécurité et de confidentialité adoptées, tant physiques que logiques.

Les destinataires des informations issues des deux traitements sont : le garde des Sceaux sur sa demande, les personnels habilités de la direction de l'administration pénitentiaire, ainsi que les agents chargés d'assurer la maintenance technique. Les services de police et de gendarmerie ne pourront recevoir que des documents papier reprenant uniquement les informations facilitant la sécurité des escortes au cours de transferts régionaux.

Délibération n° 97-054 du 30 juin 1997 portant avis conforme sur un projet de décret du ministre de la Justice portant application des dispositions de l'article 31, troisième alinéa, de la loi du 6 janvier 1978 au traitement automatisé de gestion centralisée de la population pénale mis en œuvre par la direction de l'administration pénitentiaire

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 de procédure pénale, notamment ses articles D. 77, D. 260 à D. 262, D. 280 à D. 283 et D. 290 à D. 317 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 31 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres I^{er} à III et VII de la loi du 6 janvier 1978 précitée ; Vu le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le projet de décret portant application des dispositions de l'article 31, troisième alinéa, de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au traitement automatisé d'informations nominatives de gestion centrale de la population pénale dont la direction de l'administration pénitentiaire du ministère de la Justice envisage la mise en oeuvre ;

Vu l'arrêté du 6 juin 1990 fixant l'organisation en bureaux de la direction de l'administration pénitentiaire du ministère de la Justice ;

Vu le projet d'arrêté du ministre de la Justice ;

Après avoir entendu Monsieur Michel Bernard, 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 portant application au traitement automatisé d'informations nominatives de gestion centrale de la population pénale dont la direction de l'administration pénitentiaire du ministère de la Justice envisage la mise en œuvre des dispositions de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Considérant que l'article 31 de la loi du 6 janvier 1978 interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de l'intéressé, des données nominatives faisant apparaître directement ou indirectement les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les moeurs des personnes ;

Considérant que l'article 31, troisième alinéa, de la loi précitée prévoit qu'il peut être fait exception à cette interdiction pour des motifs d'intérêt public, sur proposition ou avis conforme de la Commission, par décret en Conseil d'État ; qu'en l'espèce, ces motifs doivent être appréciés au regard des missions dévolues au ministère de la Justice ;

Considérant que le traitement de gestion centralisée de la population pénale mis en œuvre par le ministère de la Justice, a pour objet d'améliorer les conditions de prise en charge des détenus et de la gestion des établissements pénitentiaires par la centralisation des informations permettant une affectation mieux adaptée des détenus au sein de ces établissements et de faciliter les transferts d'un établissement à un autre, ainsi que la production de statistiques non nominatives ;

Considérant qu'au nombre des informations collectées peut figurer, pour les besoins exclusifs de l'affectation des détenus, de la sécurité des établissements pénitentiaires et de celle des transfèrements, l'appartenance des détenus à une organisation criminelle sous la forme d'un code ; que cette information est susceptible de faire apparaître indirectement leurs opinions politiques, philosophiques ou religieuses ;

Considérant que des motifs d'intérêt public justifient qu'il soit fait application de l'article 31, troisième alinéa, de la loi du 6 janvier 1978 pour les informations enregistrées dans le traitement qui font apparaître, directement ou indirectement, les opinions politiques, philosophiques ou religieuses des personnes ;

Émet un avis conforme sur le projet de décret en Conseil d'État portant application des dispositions de l'article 31, troisième alinéa, de la loi du 6 janvier 1978 au traitement automatisé d'informations nominatives de gestion centrale de la population pénale dont la direction de l'administration pénitentiaire du ministère de la Justice envisage la mise en œuvre.

Délibération n° 97-055 du 30 juin 1997 portant avis sur un projet d'arrêté du ministre de la Justice relatif à la création d'un traitement automatisé de données nominatives destiné à assurer la gestion centralisée de la population pénale « GCPP » (Demande d'avis n° 497 156)

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 de procédure pénale, notamment ses articles D. 77, D. 260 à D. 262, D. 280 à D. 283 et D. 290 à D. 317 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 31 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres I^{er} à III et VII de la loi du 6 janvier 1978 précitée ;

Vu la loi n° 87-432 du 22 juin 1987 relative au service public pénitentiaire ;

Vu le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le projet de décret portant application des dispositions de l'article 31, troisième alinéa, de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au traitement automatisé d'informations nominatives de gestion centralisée de la population pénale dont la direction de l'administration pénitentiaire du ministère de la Justice envisage la mise en oeuvre ; Vu l'arrêté du 6 juin 1990 fixant l'organisation en bureaux de la direction de l'administration pénitentiaire du ministère de la Justice ; Vu le projet d'arrêté du ministre de la Justice ;

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

Considérant que la Commission a été saisie d'une demande d'avis relative à la création, au sein de la direction de l'administration pénitentiaire du ministère de la Justice, d'un traitement automatisé de données nominatives destiné à assurer la gestion centralisée de la population pénale (exécution des décisions pénales, maintien de la sécurité publique et réinsertion des détenus) ;

Considérant que ce traitement a pour finalité d'améliorer les conditions de prise en charge des détenus, d'assurer une meilleure gestion des établissements pénitentiaires par la centralisation des informations permettant une affectation mieux adaptée des détenus au sein de ces établissements, ainsi que de faciliter les transferts d'un établissement à un autre ; que le traitement permettra également de disposer d'états statistiques non nominatifs ;

Considérant que sa mise en oeuvre s'inscrit dans les missions assignées au service public pénitentiaire par l'article 1er de la loi du 22 juin 1987 relative au service public pénitentiaire et dans les missions du bureau de l'individua-

lisation de la direction de l'administration pénitentiaire du ministère de la Justice, telles qu'elles résultent de l'article 5 de l'arrêté du 6 juin 1990 fixant l'organisation en bureaux de la direction de l'administration pénitentiaire du ministère de la Justice ;

Considérant que les informations collectées sont l'état civil de l'intéressé, sa nationalité, le cas échéant ses noms d'emprunt, sa situation matrimoniale, ses situation et catégorie pénales (condamné ou prévenu), la nature de la procédure judiciaire appliquée (correctionnelle ou criminelle), la condamnation définitive la plus importante, sa situation au regard des mesures d'individualisation de la peine, (période de sûreté, libération conditionnelle, notamment), l'établissement pénitentiaire d'affectation de l'intéressé, sa date d'écrou initiale, les éventuelles mesures d'isolement prises à son encontre, l'indication selon laquelle, le cas échéant, l'intéressé est un détenu particulièrement signalé ou pose un problème d'affectation, l'identité de ses complices (nom, prénom et date de naissance), les réaffectations éventuelles du détenu et leurs motifs, les éventuelles hospitalisations dans un établissement de santé, les événements affectant la vie du détenu qualifiés d'incidents individuels ou collectifs (sous la forme type d'incident, lieu et date de déroulement, motif et nombre de personnes impliquées, suites à donner, ainsi que, le cas échéant, les nom et prénoms des victimes), enfin le signalement des détenus dangereux dont la présence en détention est susceptible de causer un trouble à l'ordre public ;

Considérant qu'en application de l'article 31, troisième alinéa, de la loi du 6 janvier 1978, le ministère de la Justice envisage en outre de collecter et de conserver, pour les besoins exclusifs de l'affectation des détenus, de la sécurité des établissements pénitentiaires et de celle des transfèrements, l'appartenance éventuelle des détenus à un mouvement terroriste ou une organisation criminelle sous la forme d'un code ; que cette information étant susceptible de faire apparaître leurs opinions politiques, philosophiques ou religieuses, le ministère de la Justice a en conséquence élaboré un projet de décret en Conseil d'État faisant application des dispositions de l'article 31, troisième alinéa de la loi du 6 janvier 1978 au traitement projeté ;

Considérant que ces informations apparaissent pertinentes au regard de la finalité assignée au traitement ;

Considérant que les destinataires des informations traitées sont le garde des Sceaux sur sa demande et les personnels de la direction de l'administration pénitentiaire énumérés au projet d'arrêté portant création du traitement, et ce en fonction de leur degré d'habilitation (le directeur et son adjoint, le sous-directeur de l'exécution des décisions judiciaires et les fonctionnaires du bureau d'ordre de cette sous-direction, les magistrats, fonctionnaires et agents du bureau de l'individualisation de peines et des régimes de détention) ; que pourront également avoir accès aux informations traitées les agents du bureau de l'informatique et de l'organisation de l'administration pénitentiaire chargés d'assurer la maintenance du traitement ;

Considérant que les informations traitées sont effacées cinq années à compter de la date de levée d'écrou, à l'exception des informations relatives à l'identité des détenus (nom, prénom, date de naissance, sexe, alias éventuels et nationalité), qui sont effacées dix années après la libération ; que ces durées ne sont pas excessives par rapport aux finalités du traitement ;

Considérant que ce traitement intéresse la sûreté de l'État et la sécurité publique au sens de l'article 39 de la loi du 6 janvier 1978 ; qu'en conséquence, le droit d'accès aux informations traitées s'exercera par l'intermédiaire de la Commission, conformément à ces dispositions ;
Considérant qu'en application de l'article 26 de ladite loi le projet d'arrêté portant création du traitement exclut la possibilité pour les personnes intéressées de s'opposer à ce que les données les concernant fassent l'objet d'un traitement automatisé ;

Considérant que l'article 3 de l'arrêté dispose que « l'administration pénitentiaire rend compte chaque année à la Commission nationale de l'informatique et des libertés de ses activités de vérification, de mise à jour et d'apurement de son fichier » ; qu'il conviendrait de compléter cet article pour préciser que les modalités de ces activités seront définies en accord avec la Commission ;

Émet un avis favorable à la création, par le ministère de la Justice, d'un traitement automatisé de données nominatives destiné à assurer la gestion centralisée de la population pénale sous réserve que le dernier alinéa de l'article 3 soit complété par ces mots : « selon des modalités définies en accord avec la Commission ».

Délibération n° 97-056 du 30 juin 1997 portant avis sur un projet d'arrêté du ministre de la Justice concernant la création d'un modèle type de traitement de gestion régionale de la population pénale « GRPP »

(Demande d'avis **n°** 492 435)

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 de procédure pénale, notamment ses articles D. 260 à D. 262, D. 280 à D. 283 et D. 290 à D. 317 ;

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

Vu la loi n° 87-432 du 22 juin 1987 relative au service public pénitentiaire ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres I^{er} à III et VII de la loi du 6 janvier 1978 précitée ;

Vu le projet d'arrêté du ministre de la Justice ;

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

Considérant que la Commission a été saisie d'une demande d'avis relative à la création d'un modèle type de traitement automatisé de données nominatives destiné à assurer la gestion régionale de la population pénale (exécution des décisions pénales, maintien de la sécurité publique et réinsertion des détenus) ;

Considérant que ce traitement a pour finalité d'améliorer les conditions de prise en charge des détenus, d'assurer une meilleure gestion des établisse-

ments pénitentiaires par la centralisation au niveau régional des informations permettant d'assurer une affectation mieux adaptée des détenus au sein de ces établissements et de faciliter les transferts d'un établissement à un autre ; que le traitement permettra également de disposer d'états statistiques non nominatifs ;

Considérant que sa mise en œuvre s'inscrit dans les missions assignées au service public pénitentiaire par l'article 1er de la loi du 22 juin 1987 relative au service public pénitentiaire ;

Considérant que les informations collectées sont l'état civil de l'intéressé, sa nationalité, le cas échéant ses noms d'emprunt, sa situation matrimoniale, ses situation et catégorie pénales (condamné ou prévenu), la nature de la procédure judiciaire appliquée (correctionnelle ou criminelle), la condamnation définitive la plus importante, sa situation au regard des mesures d'individualisation de la peine, (période de sûreté, libération conditionnelle, notamment), l'établissement pénitentiaire d'affectation de l'intéressé, sa date d'écrou initiale, les éventuelles mesures d'isolement prises à son encontre, l'indication selon laquelle, le cas échéant, l'intéressé est un détenu particulièrement signalé ou pose un problème d'affectation, l'identité de ses complices (nom, prénom et date de naissance), les réaffectations éventuelles du détenu et leurs motifs, les éventuelles hospitalisations dans un établissement de santé et les événements affectant la vie du détenu qualifiés d'incidents individuels ou collectifs (sous la forme type d'incident, lieu et date de déroulement, motif et nombre de personnes impliquées, suites à donner, ainsi que, le cas échéant, les nom et prénoms des victimes) ;

Considérant que ces informations apparaissent pertinentes au regard de la finalité assignée au traitement ;

Considérant que les destinataires des informations traitées sont le garde des Sceaux sur sa demande, le directeur de l'administration pénitentiaire, les directeurs régionaux des services pénitentiaires ainsi que leurs adjoints, les chefs et agents habilités des départements de gestion des personnes placées sous main de justice des directions régionales des services pénitentiaires, ainsi que les agents des unités informatiques de ces mêmes directions afin d'assurer la maintenance du traitement ;

Considérant que les informations traitées sont effacées cinq années à compter de la date de levée d'écrou, à l'exception des informations relatives à l'identité des détenus (nom, prénom, date de naissance, sexe, alias éventuels et nationalité), qui sont effacées dix années après la libération ; que ces durées ne sont pas excessives par rapport aux finalités du traitement ;

Considérant que ce traitement intéresse la sûreté de l'État et la sécurité publique au sens de l'article 39 de la loi du 6 janvier 1978 ; qu'en conséquence, le droit d'accès aux informations traitées s'exercera par l'intermédiaire de la Commission, conformément à ces dispositions ; qu'il conviendrait toutefois que l'article 5 du projet d'arrêté soit modifié de façon à ce qu'il apparaisse que ce droit d'accès s'exerce par l'intermédiaire de la Commission ;

Considérant qu'en application de l'article 26 de ladite loi le projet d'arrêté portant création du traitement exclut la possibilité pour les personnes intéressées de s'opposer à ce que les données les concernant fassent l'objet d'un traitement automatisé ;

Émet un avis favorable à la création, par le ministère de la Justice, d'un traitement automatisé de données nominatives destiné à assurer la gestion régionale de la population pénale, sous réserve qu'à l'article 5 de l'arrêté la formule « [...] auprès de la CNIL » soit remplacée par les mots « [...] par l'intermédiaire de *la* CNIL ».

Chapitre 5

SANTÉ

I. L'UTILISATION DE FICHIERS À DES FINS DE SANTÉ PUBLIQUE

Le développement, depuis ces dernières années, de dispositifs de vigilance sanitaire et d'actions de prévention incite les autorités sanitaires à recourir de plus en plus fréquemment à des fichiers administratifs, disposant d'adresses mises à jour, et permettant de retrouver plus facilement les personnes concernées afin de leur proposer, selon la situation, un examen de dépistage ou un suivi médical approprié. La commission estime que cette utilisation, à des fins de santé publique, de fichiers dont ce n'est certes pas la finalité première, est parfaitement légitime. La CNIL a ainsi été amenée à rendre, au cours de l'année 1997, plusieurs avis favorables sur des projets présentés par les autorités sanitaires.

A. Le fichier national des assurés sociaux

La CNIL a été saisie par la direction générale de la santé d'un projet d'enquête sur les cas d'infection survenus dans la clinique du sport, à Paris, entre le 1er janvier 1988 et le 31 mai 1993. En effet, il est apparu que certains des patients opérés du rachis, au cours de cette période dans cet établissement, manifestaient des symptômes d'infection par une bactérie résultant vraisemblablement d'une mauvaise désinfection du matériel chirurgical. Les pouvoirs publics ont donc souhaité mettre en place un traitement informatique de données permettant de contacter par courrier les patients concernés afin de les informer des risques encourus, de leur proposer des examens tendant à révéler d'éventuelles lésions rachidiennes et d'en contrôler les résultats.

C'est le centre de coordination de la lutte contre les infections nosocomiales de l'inter-région Paris Nord (CCLIN) qui a été chargé d'identifier et d'informer les patients concernés par un dépistage. La liste de ces patients est dressée à partir des informations recueillies directement auprès des intéressés par l'intermédiaire d'un numéro vert mis en place par la direction générale de la santé, ou fournies par la clinique du sport à partir des dossiers médicaux de ses patients. Par ce biais, il est proposé de pratiquer un examen radiologique du rachis et de communiquer les résultats par retour de courrier au CCLIN dans une enveloppe libre-réponse. Le courrier est complété d'une mention relative à la mise en place d'un fichier par le CCLIN d'une part, et au droit d'accès d'autre part, ainsi que d'une lettre d'information à destination du médecin traitant et du radiologue qui pratiquera l'examen.

Cependant, le CCLIN ayant constaté que certaines adresses de patients, transmises par la clinique du sport, étaient erronées, une demande de consultation du répertoire national inter-régimes des bénéficiaires de l'assurance maladie (RNIAM) a été présentée par la direction générale de la santé, afin d'obtenir les coordonnées des organismes prestataires dont ils relèvent, puis par l'intermédiaire de ceux-ci, les adresses des patients. L'intérêt de l'utilisation de ce répertoire est de pouvoir contacter l'ensemble des patients concernés quel que soit leur régime d'appartenance. C'est la première fois, depuis sa création par l'ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins, que le RNIAM est consulté conformément aux dispositions de l'article R. 161 -37-V du code de la sécurité sociale, qui autorise son utilisation « dans l'intérêt de la santé des personnes concernées ou en raison du risque de maladie transmissible, par un arrêté du ministre chargé de la Santé, pris sur avis de la Commission nationale de l'informatique et des libertés » (cf. 17^{e} rapport, p. 261).

Dès lors, la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) qui assure la gestion technique du RNIAM a pu, sur la base des informations communiquées par le CCLIN (numéro de sécurité sociale, nom et prénoms, date et lieu de naissance), consulter le répertoire et obtenir les coordonnées de l'organisme d'assurance maladie. Elle a ensuite contacté chaque organisme pour obtenir les adresses et les retransmettre au CCLIN. En effet, la CNAVTS a indiqué par courrier qu'elle transmettait directement au CCLIN les adresses des patients, après avoir elle-même contacté chaque caisse par l'intermédiaire du répertoire national afin d'obtenir l'adresse de l'assuré. Concrètement, les organismes contactés par la CNAVTS complètent les listes de patients qui leur sont transmises par les adresses, avant de les renvoyer sur support papier ou sur disquette à un interlocuteur nommément désigné, sous pli « urgent et confidentiel ». Après vérification, les listes sont adressées au CCLIN par porteur. En toute hypothèse, la CNIL a exigé que les patients soient parfaitement informés de la procédure retenue pour les retrouver et, sous cette réserve, a donné un avis favorable au projet d'arrêté présenté par le secrétariat d'État à la Santé.

Délibération n° 97-094 du 2 décembre 1997 relatif à un projet d'arrêté présenté par le secrétariat d'État à la santé :

— D'une part, à la création par le Centre de coordination de la lutte contre les infections nosocomiales de l'inter-région Paris Nord d'un traitement automatisé d'informations nominatives ayant pour finalité de mener une enquête sur les cas d'infection à mycobactérium xénopi survenus dans la clinique du sport entre le 1er janvier 1988 et le 31 mai 1993 afin d'identifier et d'informer les patients sur un dépistage d'éventuelles lésions rachidiennes

— D'autre part, à l'utilisation du répertoire national interrégimes des bénéficiaires de l'assurance maladie à des fins de recherche des personnes perdues de vue opérées à la clinique du sport entre le 1er janvier 1988 et le 31 mai 1993

(Demande d'avis n° 543 691)

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 de la santé publique ;

Vu le code de la sécurité sociale, notamment ses articles L. 161-32 et R. 161-37-IV;

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

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

Vu l'arrêté du 3 août 1992 relatif à l'organisation de la lutte contre les infections nosocomiales ;

Vu le projet d'arrêté présenté par le secrétaire d'État à la santé ;

Après avoir entendu Monsieur Jean-Pierre Michel en son rapport et Madame Charlotte-Marie Pitrat, en ses observations ;

Considérant que la CNIL est saisie par le secrétariat d'Etat à la santé d'un projet d'arrêté relatif à la création par le Centre de coordination de la lutte contre les infections nosocomiales de l'inter-région Paris Nord d'un traitement automatisé d'informations nominatives ayant pour finalité de mener une enquête sur les cas d'infection à mycobactérium xénopi survenus dans la clinique du sport entre le 1er janvier 1988 et le 31 mai 1993 afin d'identifier et d'informer les patients sur un dépistage d'éventuelles lésions rachidiennes ; que cet arrêté prévoit également l'utilisation du répertoire national interrégimes des bénéficiaires de l'assurance maladie à des fins de recherche des personnes perdues de vue opérées à la clinique du sport au cours de cette période ;

Considérant en effet qu'à la suite de cas d'infections à mycobactérium xénopi survenus dans la clinique du sport à Paris entre le 1er janvier 1988

et le 31 mai 1993, le ministère de la Santé a pris la décision de diligenter une enquête auprès de tous les patients ayant subi une intervention sur le rachis dans cet établissement, et en a confié la responsabilité au Centre de coordination de la lutte contre les infections nosocomiales de l'inter-région Paris Nord ;

Considérant qu'à partir des informations recueillies soit directement auprès des patients par l'intermédiaire du numéro vert mis en place par la direction générale de la santé, soit fournies par la clinique du sport à partir des dossiers médicaux, le Centre de coordination de la lutte contre les infections nosocomiales adresse un courrier aux patients concernés les informant des finalités de l'enquête et des risques éventuels d'infection par la bactérie auxquels ils ont pu être exposés ; que ce courrier propose en conséquence aux patients de pratiquer un examen radiologique spécialisé du rachis par imagerie à résonance magnétique (IRM) et de communiquer les résultats avec l'aide de leur radiologue, par retour de courrier, au CCLIN dans une enveloppe libre-réponse ;

Considérant que les informations collectées, objet du traitement automatisé, sont les suivantes : nom, prénoms, date et lieu de naissance, type et date d'intervention à la clinique du sport, centre de radiologie choisi pour effectuer l'imagerie à résonance magnétique, résultats de l'examen et coordonnées du médecin traitant ;

Considérant que, s'agissant des personnes dont l'adresse est inexacte ou erronée, le numéro de sécurité sociale sera enregistré par le CCLIN qui, disposant des nom et prénoms des personnes concernées, interrogera le répertoire national interrégimes de l'assurance maladie géré par la caisse nationale d'assurance vieillesse des travailleurs salariés et institué par l'ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ; que l'article 2 du décret du 12 septembre 1996 pris en application de l'ordonnance précitée (article R. 161-37-V du code de la sécurité sociale) dispose que « l'utilisation du répertoire national interrégimes des bénéficiaires de l'assurance maladie à des fins de recherche des personnes est interdite en dehors des cas expressément prévus par la loi. Toutefois, une telle utilisation peut être autorisée, dans l'intérêt de la santé des personnes concernées ou en raison du risque de maladie transmissible, par un arrêté du ministre chargé de la Santé, pris sur avis de la Commission nationale de l'informatique et des libertés » ;

Considérant que cette enquête présente un intérêt de santé publique et que dès lors l'utilisation du répertoire national interrégimes est en l'espèce légitime ;

Considérant que ce répertoire comporte notamment, pour chaque bénéficiaire les informations suivantes : son numéro d'inscription au répertoire national d'identification des personnes physiques, son nom patronymique, son nom d'usage, le cas échéant ses prénoms, ses date et lieu de naissance, le cas échéant, la mention du décès ou l'indication que la personne n'est plus bénéficiaire de l'assurance maladie, l'identifiant de l'organisme d'assurance maladie qui lui sert ses prestations de base et la date de son rattachement ; que cette dernière information permettra d'obtenir auprès des caisses, selon des modalités qui devront être portées à la connaissance de la Commission, l'indication de l'adresse de la personne ; que, dès l'obten-

tion de celle-ci, le numéro de sécurité sociale sera supprimé de la base de données du CCLIN ;

Considérant toutefois que les patients dont l'adresse aura été ainsi obtenue devront être informés de la procédure ayant permis de les retrouver ;

Considérant que les données collectées sont pertinentes au regard de la finalité du traitement et que les mesures de sécurité destinées à en garantir la confidentialité sont satisfaisantes ;

Émet un avis favorable au projet d'arrêté présenté par le Secrétariat d'État à la santé sous réserve que les patients dont l'adresse sera obtenue par consultation du Répertoire soient clairement informés de la procédure ayant permis de les retrouver ;

Demande à être informée des modalités selon lesquelles ces personnes auront été contactées.

B. Les fichiers d'EDF-GDF

Le ministère de l'Intérieur a saisi la CNIL d'une demande d'avis relative à un modèle de traitement automatisé que les préfets pourront mettre en œuvre pour orchestrer une opération de santé publique liée aux risques d'accidents nucléaires. Il s'agit d'informer, par courrier, les populations qui habitent au voisinage d'une installation nucléaire, de la distribution à titre préventif de boîtes de comprimés d'iode stable, lesquels sont réputés empêcher l'iode radioactif de se fixer sur la glande thyroïde. Cela concerne environ 700 000 personnes, réparties autour de vingt-trois sites dans trente-trois départements.

Ce projet impliquant des intervenants divers, tels que les services fiscaux ou des collectivités locales, la CNIL a d'emblée appelé l'attention des intéressés sur la nécessité d'agir de façon coordonnée. Aussi, un courrier a été adressé par la Commission à la direction de la sécurité civile, la direction générale de la santé et au secrétariat général du Comité interministériel de la sécurité nucléaire auprès du Premier ministre, afin de demander des précisions sur l'opération et de rappeler les obligations prévues par la loi en cas de création de traitements automatisés d'informations nominatives. Cette démarche a conduit à l'organisation d'une réunion interministérielle à l'issue de laquelle le ministère de l'Intérieur a préparé un modèle type laissant une certaine latitude aux préfets dans les modalités de constitution des traitements.

En effet, le projet finalement soumis à la CNIL donne aux préfets le choix de recourir à trois sources d'information pour l'envoi des courriers nominatifs : la liste des abonnés au téléphone expurgée des personnes inscrites sur la liste orange, les fichiers d'habitants créés par certaines communes pour l'information de leur population, et enfin le fichier des abonnés d'EDF-GDF.

L'exploitation du fichier d'EDF-GDF a été en l'espèce admise par la Commission, par dérogation à sa doctrine *(cf.* 15^{e} rapport, p. 33) ; la CNIL a en effet été particulièrement attentive au fait que l'information relative à la distribution des comprimés d'iode stable ne serait pas adressée en même temps que les factures de l'organisme responsable du traitement, mais ferait l'objet

d'un envoi spécifique. La CNIL a également relevé que l'édition des étiquettes adresses et l'envoi des courriers étaient confiés aux centres départementaux d'EDF-GDF. Enfin, la CNIL a pris acte qu'en aucun cas les fichiers ne seraient communiqués aux services préfectoraux, et que les documents expédiés se limiteraient à un courrier d'information sur les conditions d'utilisation des comprimés d'iode stable mis à disposition dans les pharmacies à titre préventif et gratuit ; mention étant faite de l'origine des informations utilisées pour l'envoi. Aucun suivi nominatif du retrait des comprimés n'ayant été prévu, il a été demandé aux préfectures d'informer les pharmaciens qu'ils n'étaient pas habilités à relever l'identité des clients retirant des comprimés d'iode stable. Dans le même sens, la CNIL a demandé que les données utilisées dans le cadre de cette opération de santé publique soient obligatoirement détruites dès la fin *des* opérations d'envoi des courriers, le projet d'arrêté portant adoption du modèle type de traitement devant être complété sur ce point. En effet, la Commission a estimé que la durée de conservation initialement fixée à trois mois ne se justifiait pas.

Sous cette réserve, un avis favorable a été rendu et les préfectures qui mettront en œuvre le traitement devront adresser à la Commission une déclaration simplifiée, qui précisera la nature du fichier source utilisé dans leur département.

Délibération n° 97-067 du 9 septembre 1997 portant avis sur un projet d'arrêté du ministère de l'Intérieur relatif aux traitements automatisés des préfectures pour l'information des personnes résidant à proximité d'une installation nucléaire sur la distribution de comprimés d'iode stable

(Demande d'avis n° 537 454)

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° 87-565 du 22 juillet 1987 relative à l'organisation de la sécurité civile, à la protection de la forêt contre l'incendie et à la prévention des risques majeurs ;

Vu l'article R. 10-1 du code des postes et télécommunications ;

Vu l'instruction du Premier ministre n° 4 483/SG en date du 10 avril 1997 relative à la distribution préventive et au stockage d'iode stable destiné aux populations voisines des installations nucléaires ;

Vu la circulaire interministérielle d'application du 30 avril 1997 ;

Vu le projet d'arrêté présenté par le ministère de l'Intérieur ;

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

Considérant que le ministère de l'Intérieur a adressé à la Commission une demande d'avis valant modèle-type, dont l'objet est d'autoriser les représentants de **l'Etat** dans les départements siège ou limitrophes d'installations nucléaires qui le souhaitent, à mettre en œuvre un traitement automatisé pour informer les foyers habitant à proximité d'une installation nucléaire, plus précisément dans la zone couverte par le plan d'urgence de l'installation, de la distribution à titre préventif et gratuit de boites de comprimés d'iode stable ;

Considérant que l'iode stable est un médicament qui empêche la fixation de l'iode radioactif sur la glande thyroïde en cas d'accident nucléaire ; que la remise de comprimés d'iode stable à chaque foyer résidant dans une commune située en tout ou partie dans le premier périmètre du plan particulier d'intervention de l'installation a été décidée par instruction du Premier ministre en date du 10 avril 1997; qu'elle est susceptible de concerner environ 700 000 personnes, réparties autour de vingt-trois sites dans trente-trois départements ;

Considérant que les traitements envisagés ont pour finalité l'envoi à l'ensemble des foyers concernés d'une lettre, dans une enveloppe personnalisée, les informant des raisons de la démarche et des conditions d'utilisation des comprimés d'iode stable mis à leur disposition dans les pharmacies d'officine ; que les documents inclus dans les courriers, notamment le bon de retrait des boites de comprimés, sont anonymes ; qu'ils mentionnent la nature du fichier utilisé pour leur envoi ;

Considérant que les catégories d'informations utilisées pour l'envoi des lettres sont les nom, prénom et adresse de leurs destinataires, à l'exclusion de toute autre indication ;

Considérant que les informations traitées pour le compte des préfectures dans le cadre de cette opération peuvent provenir de l'un des fichiers suivants, à l'exclusion de tout rapprochement entre ces sources d'informations :
— le fichier des abonnés de France Télécom, sous réserve des dispositions de l'article R. 10-1 du code des postes et télécommunications qui interdit l'utilisation, notamment à des fins de diffusion dans le public, de listes d'abonnés qui ne serait pas préalablement expurgées des personnes ins crites sur la liste orange ;
— les fichiers d'habitants mis en œuvre par les communes à des fins d'information de la population ;
— les fichiers clientèle d'EDF-GDF.

Considérant cependant, dans cette dernière hypothèse, que les étiquettes-adresse comportant les nom, prénom et adresse des habitants, sont directement éditées, à la demande du préfet, par les centres départementaux d'EDF-GDF service, qui se chargent eux-mêmes de la mise sous pli des lettres ; que les communes peuvent également souhaiter utiliser elles-mêmes leur fichier pour l'envoi des courriers d'information ; que dans ces circonstances, aucune donnée nominative n'est transmise aux services de la préfecture ;

Considérant que les fichiers constitués dans les préfectures ont pour seuls destinataires les agents habilités du service désigné par le préfet pour conduire l'opération ;

Considérant que le ministère de l'Inférieur prévoit leur *conservation* pendant trois mois ; que cette durée pourrait être excessive, dès lors qu'il n'est pas prévu que les préfectures organisent un suivi des opérations de retrait des comprimés d'iode stable, notamment par l'organisation d'un système de relances aux populations ; qu'au surplus, l'envoi de courriers individualisés ne constitue, lorsqu'il est décidé, que l'un des éléments du plan départemental d'information ; qu'il convient, en conséquence, que les informations soient détruites dès la fin des opérations d'envoi des courriers ;

Considérant que le droit d'accès s'exerce auprès du cabinet de la préfecture du département ;

Considérant que la mise en œuvre d'un traitement par une préfecture doit faire l'objet d'une déclaration à la CNIL faisant référence au présent modèle-type et précisant la nature du fichier utilisé dans le département ;

Émet un avis favorable sur le projet d'arrêté présenté par le ministère de l'Intérieur, sous réserve que le premier alinéa de l'article 2 soit complété comme suit :

« Les catégories de données utilisées pour l'envoi des courriers sont les nom, prénom et adresse des destinataires, à l'exclusion de toute autre indication. Elles sont détruites dès la fin des opérations d'envoi des courriers. »

C. Les fichiers du personnel

Après la cessation définitive d'activité d'une société créée en 1950 pour fabriquer des briquets et quelques dérivés, seize fûts de substance radioactive entreposés sur le site industriel ont été découverts fortuitement. Par ailleurs, il a été constaté la présence de 7500 tonnes de remblais où avaient été enfouis des matériaux et gravats contaminés.

Les pouvoirs publics ont aussitôt mis en place une procédure de protection du site avec l'appui de l'Office de protection contre les rayonnements ionisants (OPRI) pour évaluer les risques existants en vue du transfert et du stockage des déchets. Pour sa part, le préfet a coordonné les actions menées en direction des populations de la région et des anciens salariés de l'usine et des campagnes d'information ont été lancées.

Dans ce contexte, la Commission a été saisie d'une demande d'avis par la direction régionale du travail et de la formation professionnelle (DRTEFP) de Champagne-Ardennes qui a souhaité reconstituer le fichier des anciens salariés de l'entreprise.

Outre la nécessité d'informer les personnes, il s'agissait de réaliser une enquête destinée à déterminer le niveau d'exposition auquel pourraient avoir été soumis les anciens salariés de l'entreprise, puis de mettre en place un suivi médical post-professionnel.

Ce projet a reçu l'approbation de la CNIL qui a relevé le caractère exemplaire de la méthodologie élaborée pour assurer le suivi médical des salariés. Les anciens salariés de la société ont été identifiés par deux sources : le service médical inter-entreprise du travail qui suit tous les salariés de l'entre-

prise depuis 1980 et l'inspection du travail qui a fourni des états d'entrée et sortie de personnel depuis 1945.

Afin de préserver la confidentialité des fichiers et des dossiers médicaux détenus par le médecin du travail, le médecin inspecteur du travail et de la main d'oeuvre de la région Champagne-Ardennes a été chargé d'assurer le pilotage de cette enquête et, à ce titre, à détenir les fichiers, à superviser l'envoi et la réception des questionnaires et à analyser les résultats de l'enquête. L'OPRI devait assurer, pour sa part, l'expertise dosimétrique estimée pour chaque salarié à partir des réponses figurant sur le questionnaire rempli par le salarié, et leurs confrontations aux mesures recueillies sur le site. Les questionnaires adressés à l'OPRI par l'inspection médicale du travail de Champagne-Ardennes, ne comportaient pas les éléments d'identité du salarié qui seront effacés et remplacés par un numéro d'ordre.

En fonction des résultats de l'expertise de l'OPRI, le médecin inspecteur du travail convoquera chaque salarié en vue d'abord, de l'informer des résultats de l'enquête, du niveau d'exposition professionnelle aux radiations ionisantes à laquelle il a été soumis durant sa vie professionnelle et ensuite, de le conseiller sur le suivi médical post-professionnel adapté ainsi que, le cas échéant, sur ses droits à réparation au titre des maladies professionnelles.

D. Les fichiers fiscaux

La direction régionale des affaires sanitaires et sociales (DRASS) de la région Provence-Alpes-Côte d'Azur (PACA) a souhaité créer une base de données en vue d'une étude épidémiologique sur les risques sanitaires encourus par les habitants de la région de Salsigne (Aude). En effet, il est apparu que cette population risquait d'avoir souffert d'une exposition chronique et prolongée aux émissions chimiques d'un complexe industriel, principalement sous la forme de dépôts de déchets et d'une accumulation de résidus de pollution dans les sols et la nappe phréatique. Les résultats de l'étude devraient permettre de définir des recommandations et de prendre les mesures *ad hoc* pour limiter la contamination de la population.

Dans cette perspective, la CNIL a été saisie d'une demande d'avis relative à la création d'une base de données démographiques portant sur 10 000 personnes résidant, soit dans l'environnement du site industriel de Salsigne, soit dans quatre communes non exposées, choisies en qualité de population témoin. Au final, c'est un échantillon représentatif de 800 personnes qui devrait faire l'objet de cette étude toxico-épidémiologique transversale.

La base de données est constituée à partir de plusieurs sources d'informations, parmi lesquelles il convient de relever un fichier des foyers fiscaux élaboré à partir d'applications de l'administration fiscale, pour les vingt-quatre communes concernées. Il s'agit là de la première utilisation d'informations fiscales dans le cadre d'études épidémiologiques, que la DRASS-PACA a essentiellement motivé par le souci d'accélérer la mise en oeuvre de cette enquête

placée sous le signe de l'urgence. L'intérêt évident de cette source d'informations réside dans la possibilité de disposer de la composition exacte du foyer au regard du nombre de personnes à charge ; ainsi, l'échantillon peut être sélectionné à partir d'une base de sondage exhaustive, qui enregistrerait au maximum, l'identité et l'adresse du contribuable, le nombre de personnes à charge, le numéro de téléphone, la tranche d'âge des personnes. Un courrier doit ensuite annoncer la visite à domicile d'enquêteurs, au cours de laquelle les personnes ayant signé un formulaire de consentement seront invitées à remplir un questionnaire indirectement nominatif et à subir quelques prélèvements biologiques.

Compte tenu du contexte local de crise sanitaire et donc de l'intérêt de santé publique qui s'attache à la réalisation immédiate de l'étude, la CNIL a pris acte des conditions dans lesquelles la base de données démographiques est constituée, en particulier la levée exceptionnelle du secret fiscal. Par ailleurs, la Commission a bien relevé que les données seront traitées par les seuls personnels de la cellule inter-régionale d'épidémiologie d'intervention, aux seules fins de constituer l'échantillon représentatif, et qu'elles seront détruites à l'issue d'un délai de six mois.

II. LA MEDECINE DU TRAVAIL

A. La gestion de la médecine préventive

Le ministère de l'Intérieur a présenté à la CNIL un projet de traitement d'informations nominatives destiné à faciliter la gestion administrative des services de médecine de prévention implantés dans les préfectures. Il est naturellement prévu que l'application enregistre des informations relatives à l'identité des agents, à leur vie professionnelle, ainsi qu'aux dates de convocation. L'information des agents sur les droits qui leur sont ouverts au titre des articles 34 et 40 de la loi du 6 janvier 1978 sera mentionnée sur les convocations à des visites et fera également l'objet d'un affichage dans le service médical.

La mise en place de ce traitement ressort de l'application du décret modifié n° 82-453 du 28 mai 1982 relatif à l'hygiène et à la sécurité du travail, et de la politique de prévention médicale dans la fonction publique, qui rend obligatoire l'institution de services de médecine de prévention au sein des administrations et établissements publics concernés, notamment pour effectuer un examen médical annuel.

La Commission a émis un avis favorable au projet d'arrêté portant adoption de ce modèle national de traitement qui pourra être implanté dans chaque préfecture sans autre formalité auprès de la CNIL.

Délibération n° 97-048 du 10 juin 1997 portant avis sur le projet d'arrêté présenté par le ministère de l'Intérieur autorisant la création d'un modèle national de traitement automatisé d'informations nominatives relatif à la gestion des services de médecine de prévention
(Demande d'autorisation n° 517 344)

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 pris pour l'application des chapitres I à IV et VII de la loi du 6 janvier 1978 ;

Vu le décret modifié n° 82-453 du 28 mai 1982 relatif à l'hygiène et à la sécurité du travail ainsi qu'à la prévention médicale dans la fonction publique ;

Vu le projet d'arrêté présenté par le ministère de l'Intérieur ;

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

Considérant que le ministère de l'Intérieur a saisi la Commission d'un traitement destiné à faciliter la gestion des services de médecine de prévention institués en application du décret du 28 mai 1982 ;

Considérant qu'à cet effet le traitement a pour finalité de permettre, d'une part, la gestion du secrétariat du service, d'autre part, la transmission à la direction du personnel d'informations anonymes à des fins statistiques, notamment en vue de l'établissement du rapport annuel d'activités remis au médecin chef conseiller technique national placé auprès du sous-directeur de l'action sociale ;

Considérant que les informations enregistrées concernent, outre l'identité de l'agent (nom, prénom, patronyme, date de naissance), grade, position, affectation, téléphone du lieu de travail, catégories de personnels, date de la dernière visite médicale obligatoire, dates de convocations, examen complémentaire professionnel, bénéfice d'une surveillance médicale spéciale (SMS) ou d'une surveillance médicale particulière (SMP), fiche de préconisations et échéance de la prochaine convocation ;

Considérant que ces informations sont pertinentes et adéquates par rapport à la finalité du traitement ;

Considérant que l'accès à l'application mise en œuvre dans chaque service sur des micro-ordinateurs dédiés sera protégée par des mots de passe individuels choisis par les utilisateurs, d'une longueur minimale de cinq caractères alphanumériques ; qu'il importe de sensibiliser les utilisateurs à la nécessité d'éviter de choisir des mots de passe trop aisément identifiables ;

Considérant que les agents seront informés de l'objet de l'application, des destinataires des informations et des conditions d'exercice de leur droit d'accès, par le biais d'affiches apposées dans les services médicaux et de

mentions apposées sur les convocations ; que ces affiches et ces mentions précisent notamment que le droit d'accès aux données médicales s'exerce par l'intermédiaire d'un médecin désigné par l'intéressé, conformément aux dispositions de l'article 40 de la loi du 6 janvier 1978 ;

Considérant que, s'agissant d'un modèle national de traitement applicable à l'ensemble des préfectures, il n'y a pas lieu pour celles-ci d'accomplir les formalités préalables ; qu'en conséquence, l'article 6 du projet d'arrêté doit être supprimé ;

Émet, sous la réserve précitée, **un avis favorable** au projet d'arrêté qui lui a été présenté ;

B. La médecine du travail agricole

En application du code rural, les caisses de mutualité agricole sont responsables de l'organisation de la médecine du travail pour les salariés agricoles et les apprentis, lesquels s'y soumettent lors de leur recrutement, puis chaque année. Dans ce cadre, les services médicaux du travail détiennent des dossiers médicaux contenant notamment des informations relatives à la vaccination et aux risques professionnels et personnels (alcool, tabac, antécédents familiaux...), mais également aux éventuelles maladies professionnelles ou contagieuses.

L'application de gestion des services de médecine du travail présenté par la Caisse centrale de mutualité sociale agricole (CCMSA) doit se substituer à un dispositif ancien d'une dizaine d'années. Outre la possibilité d'éditer les convocations aux examens et les compte rendus de ceux-ci, le nouveau système informatique présente l'intérêt majeur d'intégrer le dossier médical complet.

Par ailleurs, il est prévu que la nouvelle application utilise le numéro de sécurité sociale comme critère d'identification du dossier médical et comme élément d'information pour récupérer certaines données auprès du service chargé des accidents du travail et des maladies professionnelles et du service de médecine préventive. Le recours au NIR, et non plus au matricule agricole spécifique, constitue la principale nouveauté au regard de la loi du 6 janvier 1978.

À cet égard, la CNIL a estimé que la spécificité juridique de la médecine du travail agricole étant de relever de la mission de gestion du régime de protection sociale des professions agricoles confiée aux caisses de mutualité sociale agricole (MSA), le recours au numéro de sécurité sociale pouvait être admis dans ce cas particulier.

La CNIL a donc émis un avis favorable au modèle de traitement que les caisses de MSA peuvent mettre en œuvre après avoir procédé à une déclaration de conformité auprès de la Commission. Toutefois, la CNIL a demandé à connaître les procédures d'information des personnes qui relèvent du régime agricole, en plus de la mention du droit d'accès et de ses modalités d'exercice qui doit être apposée sur les convocations aux visites de médecine du travail.

Délibération n° 97-016 du 4 mars 1997 portant avis sur le projet de décision présenté par la Caisse centrale de mutualité sociale agricole concernant un modèle type de traitement de gestion des services de médecine du travail des caisses de mutualité sociale agricole (Demande d'avis n° 466 599)

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 ;

Vu le code rural, notamment ses articles 1000-1 et suivants ;

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

Vu le décret n° 96-793 du 12 septembre 1996 relatif à l'autorisation d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques et à l'institution d'un répertoire national interrégimes des bénéficiaires de l'assurance maladie et modifiant le code de la sécurité sociale ;

Vu le décret n° 397 du 11 mai 1982 ;

Vu l'arrêté du 7 février 1986 relatif aux modèles de statuts des caisses de mutualité sociale agricole ;

Vu la délibération n° 86-24 du 25 février 1986 portant avis sur un projet de décision présenté par les caisses centrales de mutualité sociale agricole et relatif à l'informatisation des services de médecine du travail des caisses de mutualité sociale agricole ;

Vu le projet d'acte réglementaire présenté par la caisse centrale de mutualité sociale agricole ;

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

Considérant que la caisse centrale de mutualité sociale agricole met à la disposition des caisses locales, un modèle-type de traitement automatisé dont la finalité principale est de gérer la médecine du travail des ressortissants du régime agricole concernés ;

Considérant que ce traitement est destiné à remplacer une application ayant fait l'objet d'un avis favorable de la CNIL par délibération n° 86-24 du 25 février 1986 qui avait pour finalité de gérer l'édition des convocations, des compte rendus d'examens ainsi que la tenue d'un dossier médical simplifié ;

Considérant que le nouveau traitement soumis à la Commission présente des finalités identiques mais intègre désormais le dossier médical complet sur support informatique et qu'il est ainsi procédé à la collecte d'informations sur la situation médico-sociale de l'assuré ainsi que de renseignements médicaux ; que ces informations sont adéquates, pertinentes et non excessives au regard de la finalité du traitement ;

Considérant que ce traitement prévoit d'utiliser le NIR comme identifiant du dossier médical à la place du numéro de matricule agricole ;

Considérant que l'article R. 115-2 du code de la sécurité sociale issu du décret du 12 septembre 1996 autorise les organismes et administrations limitativement énumérés à l'article R. 115-1 (dont font partie les caisses de mutualité sociale agricole) à utiliser le NIR exclusivement pour les traitements mis en œuvre dans l'exercice de leurs missions de sécurité sociale ;

Considérant qu'en application des articles 1000-1 et suivants du code rural, les caisses de mutualité agricole sont responsables de l'organisation de la médecine du travail pour les salariés agricoles et apprentis ; qu'elles peuvent, soit instituer en leur sein une section de médecine du travail, soit créer une association spécialisée ;

Considérant également que l'article 4 de l'arrêté du 7 février 1986 relatif aux modèles de statuts des caisses de mutualité sociale agricole prévoit que la caisse de mutualité sociale agricole a notamment pour objet d'assurer, conformément à la législation et à la réglementation en vigueur, la gestion du régime de protection sociale et familiale des ressortissants des professions agricoles et assimilées qui comprend la médecine du travail agricole ;

Considérant en conséquence qu'eu égard aux modalités particulières d'organisation de la médecine du travail en agriculture, la gestion de ce service par les caisses de mutualité sociale agricole relève de leurs missions de sécurité sociale ;

Considérant dès lors que les caisses de mutualité sociale agricole sont autorisées par le décret du 12 septembre précité à utiliser le NIR dans les traitements de gestion de médecine du travail agricole ;

Considérant que le traitement est mis en oeuvre sur des micro-ordinateurs reliés à un serveur dédié à l'application ; qu'une connexion est prévue avec le serveur du centre informatique régional des caisses, au moyen d'un outil infocentre, afin de récupérer certaines informations : éléments d'identification, informations concernant l'emploi principal et secondaire, accidents et arrêts de travail, données administratives concernant l'entreprise ;

Considérant que chaque caisse dispose d'un serveur de sécurité permettant d'assurer l'identification et l'authentification des postes de travail et des utilisateurs ainsi que la gestion des autorisations d'accès ;

Considérant que le droit d'accès constitue l'une des garanties essentielles de la protection des individus ; qu'en conséquence, l'existence et les modalités d'exercice de ce droit, telles que prévues aux articles 34 et 40 de la loi du 6 janvier 1978, doivent être portées expressément à la connaissance des personnes concernées notamment par une mention apposée sur les convocations aux visites de médecine du travail ;

Émet un avis favorable au projet de décision relatif à l'informatisation des services de médecine du travail étant entendu que les caisses départementales et pluridépartementales de mutualité sociale agricole qui adopteront ce modèle devront présenter à la Commission une déclaration de référence audit traitement accompagnée d'un engagement de conformité aux dispositions de l'acte réglementaire national, qui devra être publié localement, ainsi qu'aux mesures de sécurité préconisées dans la présente demande d'avis ;

Demande à être saisie des mesures d'information prévues vis-à-vis des ressortissants du régime agricole concernés par ce traitement.

Chapitre 6

RECHERCHE MEDICALE

I. LA SURVEILLANCE ÉPIDÉMIOLOGIQUE DU SIDA

L'épidémie du sida nécessite une surveillance que l'évolution et l'ampleur de cette maladie conduisent sans cesse à renforcer. La CNIL s'est déjà prononcée à deux reprises sur l'informatisation des déclarations de sida avéré, qui sont devenues obligatoires en 1986, afin de recenser des informations relatives au patient lui-même (nom, prénom, date de naissance, département de domicile, sexe, date de décès, nationalité...), à la maladie (date du diagnostic, pathologie d'entrée, mode de contamination...) et aux caractéristiques de soins (cf. 9e rapport, p. 138, 16e rapport, p. 396).

En 1997, la CNIL a délivré des avis favorables concernant plusieurs mesures visant à aménager le dispositif initial de surveillance épidémiologique du sida, afin de prendre en compte, d'une part la mission confiée au Réseau national de santé publique (RNSP) en matière de sida et d'autre part, de nouveaux flux d'informations.

Ainsi, la CNIL a été saisie par le ministère du Travail et des Affaires sociales d'un projet d'arrêté qui prévoit notamment le traitement de gestion des déclarations obligatoires des cas de sida par le RNSP et l'adjonction de nouveaux items sur le formulaire de déclaration de sida. Le RNSP a pour sa part soumis à la Commission un projet de traitement des informations résultant des déclarations obligatoires que lui adressent les médecins qui diagnostiquent un cas de sida et les médecins départementaux inspecteurs de la santé. Par ailleurs, la Commission a examiné une demande d'avis, émanant de la direction générale de la santé du ministère du Travail et des Affaires sociales, qui prévoit la

transmission d'informations issues des déclarations obligatoires, non seulement aux médecins inspecteurs des directions départementales des affaires sanitaires et sociales, lesquels veulent disposer d'une application informatique de gestion et d'analyse des cas de sida dans le département, mais aussi à l'INSERM pour permettre de poursuivre une étude de cohorte sur le suivi de paramètres biologiques et cliniques chez les personnes séropositives. L'INSERM souhaite en effet connaître le devenir, au plan médical, des personnes de la cohorte qui seraient perdues de vue.

Délibération n° 97-023 du 1er avril 1997 relative à un projet d'arrêté présenté par le ministère du Travail et des Affaires sociales relatif à l'informatisation des déclarations obligatoires de sida avéré

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 de la santé publique, et notamment, l'article L. 11 ;

Vu la loi 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 susvisée ;

Vu le décret n° 86-770 du 10 juin 1986 relatif à la liste des maladies à déclaration obligatoire ;

Vu l'arrêté du 31 octobre 1988 relatif à l'informatisation des déclarations obligatoires de sida avéré ;

Vu l'arrêté du 17 juin 1992 portant approbation de la Convention constitutive du réseau national de santé publique ;

Vu les délibérations de la CNIL n° 88-91 et 95-101 en date respectivement du 6 septembre 1988 et 11 juillet 1995 ;

Vu la délibération n° 97-024 du 1er avril 1997 relative à l'informatisation des déclarations obligatoires du sida ;

Vu le projet d'arrêté présenté par le ministère du Travail et des Affaires sociales ;

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

Considérant que la direction générale de la santé du ministère du Travail et des Affaires sociales soumet à la CNIL un projet d'arrêté fixant le contenu des déclarations obligatoires de sida ainsi que les modalités d'exploitation et de transmission des données figurant sur ces déclarations ;

Considérant en effet que la mission de surveillance épidémiologique du sida est confiée au réseau national de santé publique (RNSP) depuis une Convention du 28 juillet 1993 conclue entre la direction générale de la santé et le RNSP ; que pour assurer cette mission, le RNSP met en œuvre un traitement automatisé des informations indirectement nominatives figurant sur les déclarations obligatoires de sida ; que les informations contenues dans ces déclarations ont été complétées d'éléments relatifs aux critères cliniques dus à l'évolution de la pathologie du sida ;

Considérant que le projet d'arrêté précise que les praticiens déclarent, sous pli cacheté confidentiel, les cas de sida diagnostiqués auprès des médecins inspecteurs des directions départementales des affaires sanitaires et sociales qui eux-mêmes, après validation, les adressent au RNSP ; qu'il est en outre prévu que le RNSP retransmette aux médecins inspecteurs des DDASS, sur support informatique, les données relatives aux cas de sida déclarés dans le département ;

Considérant que le projet d'arrêté prévoit également que le réseau national de santé publique puisse adresser de façon ponctuelle à des équipes de recherche des données issues des déclarations obligatoires de sida et ce afin de réaliser des études épidémiologiques ; que cette communication d'informations s'effectuera dans le respect des dispositions de la loi du 1er juillet 1994 ;

Émet un avis favorable au projet d'arrêté présenté par le ministère du Travail et des Affaires sociales relatif à l'informatisation des déclarations obligatoires de sida avéré.

Délibération n° 97-024 du 1er avril 1997 relative à un projet d'arrêté présenté par la direction générale de la santé du ministère du Travail et des Affaires sociales concernant la mise en œuvre, dans chaque direction départementale des affaires sanitaires et sociales d'un traitement national de données indirectement nominatives issues des déclarations obligatoires de sida détenues par le RNSP

(Demande d'avis n° 520 468)

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 de la santé publique, et notamment, l'article L. 11 ; Vu la loi 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 susvisée ;

Vu le décret n° 86-770 du 10 juin 1986 relatif à la liste des maladies à déclaration obligatoire ;

Vu l'arrêté du 31 octobre 1988 relatif à l'informatisation des déclarations obligatoires de sida avéré ;

Vu l'arrêté du 17 juin 1992 portant approbation de la Convention constitutive du réseau national de santé publique ;

Vu les délibérations de la CNIL n° 88-91 et 95-101 en date respectivement du 6 septembre 1988 et 11 juillet 1995 ;

Vu le projet d'arrêté présenté par le ministère du Travail et des Affaires sociales ;

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

Considérant que la direction générale de la santé du ministère du Travail et des Affaires sociales met en œuvre dans chaque direction départementale des affaires sanitaires et sociales (DDASS) un traitement automatisé d'informations indirectement nominatives ayant pour objet de permettre aux

médecins inspecteurs de gérer et d'analyser les cas de sida propres au département ;

Considérant que le médecin inspecteur joue un rôle important dans la surveillance épidémiologique du sida puisqu'il lui appartient d'effectuer un premier contrôle de validité des données qui lui sont transmises par les cliniciens, et qu'il adresse ensuite, sous pli médical confidentiel, au médecin épidémiologiste chargé du dossier au RNSP ; qu'en retour, le médecin inspecteur de la DDASS informe les cliniciens et leur diffuse chaque trimestre les données les plus récentes sur l'épidémie ;

Considérant que l'application proposée par la direction générale de la santé permettra aux médecins inspecteurs, à partir des données relatives aux cas de sida déclarés dans le département et transmises trimestriellement par le RNSP, de procéder à leur exploitation épidémiologique et d'assurer ensuite la diffusion de statistiques départementales auprès des médecins du département ;

Considérant que les informations issues des déclarations obligatoires des cas de sida et traitées au niveau départemental par les directions départementales des affaires sanitaires et sociales sont les mêmes que celles traitées au niveau national par le RNSP ; qu'aucune donnée supplémentaire ne sera traitée au niveau départemental ; que les seuls résultats produits par ce traitement sont des statistiques globales ;

Considérant que les données indirectement nominatives transmises sur disquettes par le RNSP seront codées et compressées ; qu'en outre, l'accès à l'application est protégé par une procédure de mots de passe ;

Considérant que le droit d'accès aux données détenues par les DDASS s'exerce auprès du RNSP par l'intermédiaire du médecin déclarant ; que le RNSP reste dans tous les cas l'organisme auprès duquel s'exerce le droit d'accès ;

Émet un avis favorable au projet d'arrêté présenté par la direction générale de la santé du ministère du Travail et des Affaires sociales concernant la mise en oeuvre, dans chaque direction départementale des affaires sanitaires et sociales d'un traitement national de données indirectement nominatives issues des déclarations obligatoires de sida détenues par le réseau national de santé public.

Délibération n° 97-025 du 1er avril 1997 relative à un projet d'acte réglementaire présenté par le réseau national de santé publique concernant un traitement automatisé d'informations indirectement nominatives ayant pour finalité la surveillance de l'épidémie de sida à partir des déclarations obligatoires des cas de sida (Demande d'avis n° 494 968)

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 de la santé publique, et notamment, l'article L. 11 ;

Vu la loi 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 susvisée ;

Vu le décret n° 86-770 du 10 juin 1986 relatif à la liste des maladies à déclaration obligatoire ;

Vu l'arrêté du 31 octobre 1988 relatif à l'informatisation des déclarations obligatoires de sida avéré ;

Vu l'arrêté du 17 juin 1992 portant approbation de la Convention constitutive du réseau national de santé publique ;

Vu les délibérations de la CNIL n° 88-91 et 95-101 en date respectivement du 6 septembre 1988 et 11 juillet 1995 ;

Vu la délibération n° 97 023 du 1er avril 1997 relative à l'informatisation des déclarations obligatoires de sida ;

Vu le projet d'acte réglementaire présenté par le réseau national de santé publique ;

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

Considérant que le réseau national de santé publique (RNSP), groupement d'intérêt public créé par arrêté du 17 juin 1992, a saisi la CNIL d'un projet d'acte réglementaire relatif à un traitement automatisé d'informations indirectement nominatives ayant pour finalité la surveillance épidémiologique du sida à partir des déclarations obligatoires de sida ;

Considérant que le RNSP est chargé depuis une Convention du 28 juillet 1993 conclue avec la direction générale de la santé du ministère du Travail et des Affaires sociales, de la mission de surveillance épidémiologique du virus du sida ;

Considérant que le traitement automatisé mis en œuvre par le RNSP a pour finalité l'analyse des déclarations obligatoires de sida, la description de l'épidémie, l'étude des modes de transmission et la définition des décisions en matière de santé publique ;

Considérant que les informations traitées par le RNSP proviennent des formulaires de déclaration obligatoire qui lui sont adressés, sous pli confidentiel, par les médecins inspecteurs de la santé dans chaque département qui les a reçus du praticien ayant diagnostiqué un cas de sida ; que ces données portent sur les initiales du nom et du prénom, la date de naissance et le département de domicile, le sexe, la date de décès, le département de naissance et le pays de domicile, la nationalité et la catégorie socioprofessionnelle ; que le traitement collecte également les données relatives au diagnostic du sida et aux caractéristiques de soins ;

Considérant que les destinataires de ces données sont les personnes directement affectées à la surveillance épidémioiogique du sida au sein de l'unité de maladies infectieuses du RNSP ; qu'il est en outre prévu la possibilité de transmettre des données à des organismes de recherche autorisés à les traiter dans le respect des dispositions de la loi du 6 janvier 1978 ; qu'ainsi, il est prévu de transmettre à l'unité 292 de l'INSERM qui étudie depuis 1987 les paramètres biologiques et cliniques d'une cohorte de personnes séropositives infectées par le sida des informations sur le devenir des personnes « perdues de vue » ; qu'à cet effet, l'INSERM adresserait au RNSP pour chacune des personnes de la cohorte les données relatives à la date de naissance, au sexe, à la date de la première sérologie positive et au groupe de transmission ; que sur la base de ces informations, le RNSP retransmettrait à l'INSERM les informations sur la date de passage au stade sida de la

maladie, la pathologie diagnostiquée à l'origine, le groupe de transmission, la survenue et la date du décès éventuellement ;

Considérant que cette procédure de transmission, qui ne porte que sur des données indirectement nominatives, serait suivie environ une fois tous les deux ans présente un intérêt de santé publique évident et ne soulève pas d'observations particulières ;

Considérant qu'il est également prévu que le RNSP transmette régulièrement au médecin inspecteur chargé de la surveillance des maladies transmissibles dans chaque direction départementale des affaires sanitaires et sociales une disquette contenant les données individuelles des déclarations de son département ; que les données contenues dans les disquettes font l'objet d'une codification et d'une compression qui assurent leur confidentialité ; Considérant que le droit d'accès aux données figurant dans le fichier national des cas de sida déclarés s'exerce auprès au RNSP, par l'intermédiaire du, médecin déclarant ;

Émet un avis favorable au projet d'acte réglementaire présenté par le Réseau national de santé publique concernant le traitement automatisé d'informations indirectement nominatives ayant pour finalité la surveillance épidémiologique du sida.

II. LES DEMANDES D'AUTORISATION PRÉVUES PAR LA LOI DU 1er JUILLET 1994

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 de protection pour les fichiers de recherche en santé. Cette levée partielle du secret médical est compensée par la reconnaissance d'un certain nombre de droits aux personnes concernées, qui doivent être informées individuellement de l'objet de la recherche, de la nature des données traitées, des destinataires, des conditions d'exercice de leurs droits d'accès et de rectification, ainsi que de leur possibilité de s'opposer au traitement des informations les concernant sans devoir justifier de raisons légitimes. De plus, leur consentement doit être recueilli en cas de recherche faisant appel à des prélèvements biologiques identifiants.

La loi prévoit toutefois des possibilités de dérogation, sous contrôle de la CNIL, à cette obligation d'information, d'une part lorsque le médecin estime, pour des raisons légitimes, que le malade doit être laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave et, d'autre part, lorsque les données ont été recueillies initialement pour un autre objet que la recherche et qu'il est désormais difficile de retrouver les personnes concernées.

En contrepartie, cette loi a renforcé les procédures de contrôle sur ces fichiers, dont la création devra être autorisée 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 *[cf.* 15e rapport d'activité, p. 27).

Le décret d'application du 9 mai 1995 a précisé la composition et le fonctionnement de ce comité consultatif, a défini la procédure d'instruction des demandes d'avis devant ce comité ainsi que celle des demandes d'autorisation devant la CNIL et, enfin, a détaillé les modalités d'information des personnes concernées par ces traitements automatisés (cf. 16e rapport, p. 23).

En 1997, la Commission a donc commencé à se prononcer sur des dossiers dont le Comité avait été préalablement saisi. Parallèlement, la CNIL a élaboré un formulaire de demande d'autorisation qui simplifie les formalités incombant aux organismes de recherche *[cf. supra 1*re partie, chapitre 1).

A. Les demandes de dérogation à l'obligation d'information individuelle

1) LES RECHERCHES SUR LE RISQUE DE MORTALITÉ DES SALARIÉS

Conformément aux dispositions de l'article 40.2 de la loi du 6 janvier 1978 modifiée, et après un avis favorable du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, la CNIL a été saisie de deux demandes d'autorisation concernant la mise en œuvre de recherches destinées à évaluer le risque de mortalité des salariés dans certains secteurs d'activité. L'une a été présentée par l'INSERM qui a été chargé, à la demande du syndicat européen de l'industrie routière, de réaliser une étude épidémiologique de la mortalité par cancer des travailleurs exposés aux fumées de bitume. L'autre est conduite par le centre de recherche en santé-travail-ergonomie de Lille qui, à la demande du Comité d'hygiène, de sécurité et des conditions de travail de l'usine Rhône-Poulenc Biochimie d'Elbeuf, a été chargé par le groupe Rhône-Poulenc, d'effectuer une enquête épidémiologique de mortalité sur ce site.

Dans les deux cas, les fichiers du personnel des entreprises concernées sont utilisés pour recenser les informations relatives aux salariés et constituer une cohorte, puis rechercher si les personnes sont vivantes ou décédées. Afin de procéder à une analyse comparative globale entre les salariés actuellement dans l'entreprise avec les anciens salariés, le cas échéant décédés, les deux organismes de recherche doivent disposer non seulement des caractéristiques de la population salariée, mais également de l'identité des personnes qui ne se trouvent plus dans l'entreprise ; il s'agit en effet de savoir si au moment de l'étude celles-ci sont mortes ou vivantes, informations qui peuvent être obtenues auprès des mairies de naissance, lesquelles sont tenues de délivrer à tout requérant des extraits d'acte de naissance.

La recherche des causes de décès est toujours réalisée en collaboration avec le service commun n° 8 de l'INSERM, service d'information sur les causes

médicales de décès, et chargé à ce titre de l'exploitation statistique des certificats médicaux de décès qui sont obligatoirement établis lors de tout décès.

Les deux demandes d'enquête présentaient également l'analogie de comporter une demande de dérogation à l'obligation d'information individuelle des personnes concernées par la recherche, formulée sur le fondement de l'article 40.5 dernier alinéa de la loi du 6 janvier 1978 et motivée par la difficulté à effectuer cette information auprès des personnes ayant quitté l'entreprise, a fortiori si elles sont décédées.

Cet article dispose que : « 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.... 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.... ». En l'occurrence, la CNIL a estimé que l'absence d'information individuelle ne se justifiait qu'à l'égard des personnes ayant quitté l'entreprise. Aussi, l'autorisation de mise en œuvre de ces deux enquêtes épidémiologiques de mortalité des salariés a été délivrée dans les strictes conditions d'une dérogation partielle à l'obligation d'information individuelle des personnes.

Délibération n° 97-042 du 27 mai 1997 portant autorisation de mise en œuvre par l'INSERM (unité 170) d'un traitement automatisé d'informations nominatives ayant pour finalité une étude épidémiologique de la mortalité des travailleurs exposés aux fumées de bitume
(Demande d'autorisation n° 518 473)

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 ses articles 40.2, 40.4 et 40.5 ; Vu le décret n° 78-774 du 17 juillet 1978 modifié par le décret n° 95-682 du 9 mai 1995 pris pour l'application de la loi susvisée ; Vu l'avis favorable rendu 18 avril 1997 par le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ; Vu la demande d'autorisation présentée par le directeur général de l'INSERM ; Après avoir entendu Monsieur Jean-Marie Poirier, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ; Considérant que l'INSERM a saisi la Commission d'une demande d'autorisation portant sur la mise en œuvre, sous la responsabilité d'un chercheur de l'unité de recherche 170 « recherches épidémiologiques et statistiques sur l'environnement et la santé », d'un traitement automatisé d'informations nominatives ayant pour finalité une étude épidémiologique de la mortalité des travailleurs exposées aux fumées de bitume ;

Considérant que cette étude, réalisée dans le cadre d'une recherche multicentrique internationale coordonnée par le Centre international de recherche sur le cancer, a pour objet d'évaluer auprès d'une cohorte de personnes effectuant des travaux de revêtement routiers, le risque de mortalité par cancer ainsi que les facteurs de risques ;

Considérant que les objectifs de cette recherche revêtent un intérêt de santé publique ;

Considérant que l'étude consiste à recueillir, à partir des fichiers de personnel tenus dans deux entreprises de travaux routiers, pour chaque salarié présent dans l'entreprise en 1980 ou embauché depuis, les informations suivantes : nom, prénom, numéro de la commune de naissance (inclus dans le numéro de sécurité sociale enregistré dans le fichier de paie), date de naissance, date d'embauche et de sortie de l'entreprise, intitulé des postes occupés aux différentes périodes dans l'entreprise ; que l'identité, la date et la commune de naissance permettront à l'INSERM d'obtenir auprès des mairies de naissance l'indication du décès et de la date de survenue de celui-ci ; que ces informations, à l'exclusion du nom, permettront ensuite de rechercher la cause médicale du décès auprès du service d'information sur les causes médicales de décès chargé de l'exploitation statistique nationale des certificats médicaux de décès ; que l'unité 170 de l'INSERM procédera ensuite à l'analyse statistique des informations ainsi obtenues ;

Considérant qu'en fonction des résultats produits l'étude sera, le cas échéant, poursuivie afin de recueillir des informations complémentaires sur les facteurs de risque ; que cette deuxième phase d'étude fera l'objet d'une demande d'autorisation auprès de la CNIL ;

Considérant que les données recueillies dans le cadre de la première phase de recherche sont pertinentes au regard des finalités poursuivies ;

Considérant que les données relatives aux salariés ayant quitté l'entreprise doivent être recueillies et conservées sous une forme nominative jusqu'à la fin de l'étude pour permettre, d'une part, de recueillir auprès des mairies de naissance l'indication du décès et, d'autre part, de collecter des données complémentaires sur les facteurs de risque ;

Considérant qu'il sera procédé à l'anonymisation des données individuelles concernant les personnes actuellement salariées dans l'entreprise, transmises à l'INSERM pour lui permettre de procéder à une analyse comparative globale de cette population de salariés et de la population de personnes décédées ;

Prenant acte de ce que le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, chargé d'apprécier la méthodologie de la recherche, l'utilité du recours aux données nominatives et la pertinence des données, a émis un avis favorable à la mise en oeuvre du traitement ;

Considérant que les dispositions envisagées pour garantir la confidentialité des données sont satisfaisantes ; qu'il est en particulier prévu une séparation des données en deux fichiers distincts, l'un, accessible uniquement par le chercheur responsable de l'étude, comportant les identités, associées à des numéros d'ordre et l'indication de la commune et de la date de naissance des personnes concernées, l'autre fichier conservant les données médicales assorties de ces mêmes numéros, à l'exclusion de toute identité ;

Considérant que l'INSERM, conformément à l'article 40.5 dernier alinéa de la loi du 6 janvier 1978 modifiée, souhaite déroger à l'obligation d'informer les personnes de l'utilisation des données les concernant ;

Considérant que conformément au dernier alinéa de l'article 40.5 de la loi du 6 janvier 1978 modifiée, « 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 » ;

Considérant que, s'il y a lieu d'admettre une dérogation à l'obligation d'information individuelle pour les personnes ayant quitté l'entreprise, s'agissant des salariés présents dans l'entreprise au moment de l'étude les conditions auxquelles l'article 40.5 de la loi du 6 janvier 1978 modifiée par la loi du 1er juillet 1994 subordonne la dérogation ne peuvent être considérées comme réunies ; que dès lors les salariés présents dans l'entreprise doivent être informés de la recherche selon des modalités appropriées ;

Considérant que le Comité d'hygiène, de sécurité et des conditions de travail d'une des entreprises participant à la recherche a été informé de l'objet et des modalités de réalisation de la recherche ;

Autorise les entreprises ayant accepté de participer à l'étude et l'INSERM à ne pas procéder à une information individuelle des personnes ayant quitté l'entreprise ;

Autorise la mise en œuvre par l'INSERM du traitement automatisé de données nominatives ayant pour finalité une étude épidémiologique de la mortalité des travailleurs exposés aux fumées de bitume.

Délibération n° 97-084 du 4 novembre 1997 portant autorisation de mise en œuvre par le Centre de recherche en santé, travail, ergonomie de Lille d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique de la mortalité des salariés de l'usine Rhône-Poulenc d'Elbeuf

(Demande d'autorisation n° 997 040)

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, notamment ses articles 40.2, 40.4 et 40.5 ;

Vu le décret n° *78-774* du 17 juillet 1978 modifié par le décret n° 95-682 du 9 mai 1995 pris pour l'application de la loi susvisée ;

Vu l'avis favorable rendu le 9 juillet 1997 par le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ;

Vu la demande d'autorisation présentée par le président du Centre de recherche en santé, travail, ergonomie (CERESTE) ;

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

Considérant que le Centre de recherche en santé, travail, ergonomie de Lille a saisi la Commission d'une demande d'autorisation portant sur la mise en oeuvre, en collaboration avec le service d'épidémiologie et de santé publique de l'hôpital Calmette de Lille, d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique portant sur la mortalité des salariés de l'usine Rhône-Poulenc d'Elbeuf ;

Considérant que cette étude est réalisée sur la demande conjointe du Comité d'hygiène, de sécurité et des conditions de travail et de la direction de l'entreprise en accord avec le médecin conseil du groupe Rhône-Poulenc ; qu'elle a pour objectif, d'une part, d'évaluer la mortalité des salariés travaillant ou ayant travaillé régulièrement à l'usine Rhône-Poulenc biochimie d'Elbeuf et, d'autre part, de rechercher d'éventuelles relations entre les données d'expositions professionnelles et les données concernant le statut vital et les causes médicales individuelles de décès ;

Considérant que l'étude consiste à recueillir, à partir du fichier de gestion du personnel de l'entreprise et du fichier détenu par le service de médecine du travail, pour chaque salarié de sexe masculin de nationalité française ayant travaillé au moins 365 jours consécutifs dans l'usine d'Elbeuf, entre le 1er janvier 1969 et le 31 décembre 1995, les informations suivantes : date et lieu de naissance, dernière adresse connue, numéro de téléphone, dates d'entrée et de sortie de l'entreprise, mode de sortie, situation dans l'entreprise au 31 décembre 1995, date et lieu de décès, s'il y a lieu, historique des emplois dans l'entreprise, consommation de tabac et d'alcool, antécédents médico-chirurgicaux, statut vital ;

Considérant que les nom, prénoms, date et lieu de naissance permettant au service de médecine du travail d'obtenir auprès des mairies de naissance l'indication du décès éventuel de la personne ; que ces informations, à l'exclusion de l'identité de la personne mais accompagnée d'un numéro d'identification individuel de l'enquête permettront ensuite de rechercher la cause médicale du décès auprès du service d'information sur les causes médicales de décès chargé de l'exploitation statistique nationale des certificats médicaux de décès ; que le service d'épidémiologie de l'hôpital Calmette, en collaboration avec le service de médecine du travail, procédera ensuite à l'exploitation statistique des informations ainsi obtenues ;

Considérant que les données recueillies sont pertinentes au regard de la finalité poursuivie ; que le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, chargé d'apprécier la méthodologie de la recherche, l'utilité du recours aux données nominatives et la pertinence des données, a émis un avis favorable à la mise en oeuvre du traitement ;

Considérant que les dispositions envisagées pour garantir la confidentialité des données sont satisfaisantes ; qu'en particulier, les informations enregistrées sont indirectement nominatives, les questionnaires étant numérotés ; que la liaison entre les numéros de questionnaire et l'identité des personnes enquêtées ne sera pas informatisée et restera détenue exclusivement par le service de médecine du travail ;

Considérant que le Centre de recherche en santé, travail, ergonomie, conformément à l'article 40.5 dernier alinéa de la loi du 6 janvier 1978 modifiée, souhaite déroger à l'obligation d'informer les personnes de l'utilisation des données les concernant ;

Considérant que conformément au dernier alinéa de l'article 40.5 de la loi du 6 janvier 1978 modifiée, « 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 » ;

Considérant qu'il y a lieu d'admettre une dérogation à l'obligation d'information individuelle pour les personnes ayant quitté l'entreprise ; que les personnes encore présentes dans l'entreprise sont informées de l'enquête par une note d'information affichée au service du personnel et dans le service de médecine du travail ;

Autorise le Centre de recherche en santé, travail, ergonomie à ne pas procéder à une information individuelle des personnes ayant quitté l'entreprise ;

Autorise la mise en œuvre par le Centre de recherche en santé, travail, ergonomie du traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique portant sur la mortalité des salariés de l'usine Rhône-Poulenc d'Elbeuf.

2) LA RECHERCHE SUR LA CONTAMINATION PAR LES ANIMAUX DOMESTIQUES

La cellule inter-régionale Sud-Est d'épidémiologie et d'intervention de la direction régionale des affaires sanitaires et sociales de la région Provence-Alpes-Côte d'Azur a saisi la CNIL d'une demande d'autorisation concernant une enquête rétrospective sur six types d'affections transmises de l'animal à l'homme, dans le pourtour méditerranéen. L'incidence de ces affections, dites zoonoses, est en effet mal connue et pose un problème de santé publique, notamment au regard de la quantité importante d'animaux domestiques dans cette zone. Il s'agit donc de décrire les caractéristiques épidémiologiques, de connaître les agents responsables et leurs modes de transmission afin de fournir des éléments, pour orienter la politique vaccinale et prophylactique pour certaines de ces pathologies. Il convient de signaler que la nationalité et le pays d'origine sont collectés pour les besoins de l'enquête afin de distinguer les « cas autochtones » des « cas importés », ainsi que les zones d'endémie de ces maladies.

Le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé a émis un avis favorable à cette enquête de santé publique qui a particulièrement retenu l'attention de la Commission au plan des modalités d'information des personnes contaminées, qu'elles soient hospitalisées dans des établissements publics ou privés, ou suivies par un médecin en ville.

En effet, à la demande de la CNIL sur le fondement de l'article 40.5 de la loi du 6 janvier 1978 modifiée qui exige que le dispositif d'information des personnes soit décrit dans le dossier de demande d'autorisation, il avait été indiqué à la Commission qu'un courrier d'information serait adressé aux patients concernés par l'enquête à partir des coordonnées mentionnées dans leurs dossiers médicaux et qu'un délai de quinze jours leur serait octroyé pour manifester un droit d'opposition éventuel.

À cet égard, la CNIL a estimé que la loi devait être strictement appliquée, et qu'en conséquence, les services hospitaliers et les médecins qui détiennent les dossiers médicaux doivent informer préalablement par écrit les patients au sujet de l'enquête et des droits qui leur sont garantis, notamment pour s'assurer, avant toute collecte de données, que le patient ne s'oppose pas au traitement. Sous cette réserve, la Commission a autorisé la mise en œuvre de l'application nécessaire à la réalisation de cette recherche.

Délibération n° 97-090 du 24 novembre 1997 portant autorisation de mise en œuvre par la direction régionale des affaires sanitaires et sociales de la région Provence-Alpes-Côte d'Azur d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête d'incidence rétrospective sur six zoonoses du pourtour méditerranéen

(Demande d'autorisation n° 997 061) -

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 ses articles 40.2, 40.4 et 40.5 ; Vu le décret n° 78-774 du 17 juillet 1978 modifié par le décret n° 95-682 du 9 mai 1995 pris pour l'application de la loi susvisée ; Vu l'avis favorable rendu le 28 mai 1997 par le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ; Vu la demande d'autorisation présentée par le directeur régional des affaires sanitaires et sociales ;

Après avoir entendu Monsieur Jean-Marie Poirier, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ; Considérant que la cellule inter-régionale Sud-Est d'épidémiologie et d'intervention de la direction régionale des affaires sanitaires et sociales de la région Provence-Alpes-Côte d'Azur a saisi la Commission d'une demande d'autorisation portant sur la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête d'incidence rétrospective sur six zoonoses du pourtour méditerranéen ; Considérant que cette enquête a pour objet de procéder à une estimation des cas de brucellose, d'hydatidose, de leishmaniose viscérale, de leptos-pirose, de fièvre Q et de fièvre boutonneuse dans les différents départements du pourtour méditerranéen afin d'estimer l'incidence de ces maladies en 1995 et 1996, d'en décrire les caractéristiques épidémiologiques, de connaître les agents responsables et leurs modes de transmission et de fournir des éléments pour orienter la politique vaccinale et prophylactique ;

Considérant que les départements d'informations médicales des centres hospitaliers de la région, les laboratoires d'analyses médicales privés et publics de bactériologie et de parasitologie, les directions départementales des affaires sanitaires et sociales chargées de la gestion des déclarations obligatoires de brucellose et les centres nationaux de référence de Marseille

et Montpellier auprès desquels sont déclarés les leishmanioses et les fièvres J transmettront à la cellule d'épidémiologie et d'intervention le nombre annuel de cas recensés pour chacune des zoonoses, les services d'hospitalisation ayant eu à traiter ces cas et la date d'entrée de chaque patient ; que les organismes source précités communiqueront également, sous couvert au secret médical, aux médecins chefs de service ayant diagnostiqué des cas de zoonoses les éléments nécessaires à l'identification du dossier médical ou du séjour hospitalier des patients hospitalisés pour une des six zoonoses en 1995 et 1996 ;

Considérant que des médecins enquêteurs de la cellule d'épidémiologie recueilleront auprès des médecins chefs des services hospitaliers concernés les informations suivantes issues des dossiers médicaux : les initiales du nom et du prénom, le sexe, la date de naissance ou l'âge, la catégorie socioprofessionnelle, le code postal du domicile du patient, la nationalité et le pays d'origine, le ou les pays ayant été visités au cours des dernières années, le cas échéant la profession des parents s'il s'agit d'enfants, et l'ensemble des informations cliniques nécessaires à la description de chaque zoonose, en particulier les « co-infections » et facteurs de risque associés à chacune de ces zoonoses ;

Considérant que la recherche de doublons éventuels sera effectuée par la méthode dite de « capture-recapture » à partir des informations précitées ; que les médecins de la cellule d'épidémiologie procéderont ensuite à l'exploitation statistique des informations ainsi obtenues ;

Considérant que les données recueillies sont pertinentes au regard de la finalité poursuivie ; que le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, chargé d'apprécier la méthodologie de la recherche, l'utilité du recours aux données nominatives et la pertinence des données a émis un avis favorable à la mise en œuvre du traitement ;

Considérant que les dispositions envisagées pour garantir la confidentialité des données sont satisfaisantes ; qu'en particulier, les informations enregistrées sont indirectement nominatives, les questionnaires étant numérotés ;

Considérant que, s'agissant de l'obligation d'informer les personnes de l'utilisation des données les concernant prévus à l'article 40.5 de la loi du 6 janvier 1978 modifiée qui précise que cette information doit être effectuée avant le début du traitement, l'article 25-20-III du décret d'application de la loi prévoit que, sauf dérogation accordée par la Commission et dans le cas où les données nominatives ont été initialement recueillies pour un autre objet que le traitement automatisé envisagé, l'établissement ou le professionnel de santé détenteur des données informe *par* écrit les personnes concernées ;

Considérant qu'il n'y a pas lieu d'admettre la dérogation à l'obligation d'information et qu'il appartient donc aux services hospitaliers et aux médecins détenteurs des dossiers médicaux d'informer préalablement par écrit les patients, de l'objet de l'enquête, des modalités de sa réalisation, des droits qui leur sont garantis par la loi précitée et de s'assurer, avant toute collecte des données, que le patient ne s'oppose pas au traitement des informations le concernant ;

Autorise la mise en œuvre par la cellule d'épidémiologie de la direction régionale des affaires sanitaires et sociales de Provence-Alpes-Côte d'Azur du traitement automatisé d'informations nominatives ayant pour finalité une enquête d'incidence rétrospective sur six zoonoses du pourtour méditerra-

néen, sous réserve que les services hospitaliers et médecins concernés adressent préalablement à chaque personne concernée un courrier les informant de l'objet de l'enquête et des droits qui leur sont garantis par la loi.

B. L'originalité de la recherche sur l'asthme des enfants et les transports

La CNIL a autorisé la mise en œuvre d'un traitement d'informations nominatives utile à la réalisation d'une enquête épidémiologique sur le rôle de la pollution atmosphérique d'origine automobile dans le développement de la maladie asthmatique chez l'enfant et présentée par le laboratoire de santé publique de la faculté de médecine de Grenoble.

Cette enquête, qui a préalablement reçu un avis favorable du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, doit être conduite dans cinq agglomérations urbaines sur environ 1070 enfants de 4 à 14 ans, asthmatiques ou témoins, recrutés en milieu hospitalier.

La méthodologie et les outils utilisés pour cette étude méritent une attention particulière. En effet, pas moins de quatre questionnaires différents ont vocation à être utilisés pour le recueil des informations et de surcroît, il est prévu que chaque enfant participant à l'enquête soit équipé pendant 48 heures d'un capteur destiné à mesurer la pollution de l'air.

Au terme de la collecte, l'exploitation statistique des données doit servir à mettre en évidence un lien entre l'indice d'exposition rétrospective au trafic automobile et la mesure de l'exposition personnelle aux polluants atmosphériques.

L'information des parents concernés est parfaitement conforme aux dispositions de la loi du 6 janvier 1978 modifiée, dans la mesure où chacun se verra remettre, à l'occasion de la consultation, une note individuelle d'information précisant la finalité de l'étude, l'identité des responsables de l'enquête et les modalités d'exercice du droit d'accès. Une copie des questionnaires leur sera également fournie en vue de recueillir leur consentement sous une forme expresse.

Délibération n° 97-085 du 4 novembre 1997 portant autorisation de mise en œuvre par le laboratoire de santé publique de la faculté de médecine de Grenoble d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique sur l'asthme de l'enfant et les transports

(Demande d'autorisation n° 997 084)

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, notamment ses articles 40.2, 40.4 et 40.5 ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié par le décret n° 95-682 du 9 mai 1995 pris pour l'application de la loi susvisée ;

Vu l'avis favorable rendu le 26 septembre 1997 par le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ;

Vu la demande d'autorisation présentée par le président de la faculté de médecine de Grenoble ;

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

Considérant que le laboratoire de santé publique de la faculté de médecine de Grenoble a saisi la Commission nationale de l'informatique et des libertés, conformément aux dispositions de l'article 40.2 de la loi du 6 janvier 1978 modifiée, d'une demande d'autorisation concernant une enquête épidémiologique de type cas-témoins sur le rôle de la pollution atmosphérique d'origine automobile dans le développement de la maladie asthmatique de l'enfant ; que cette enquête sera conduite dans les agglomérations urbaines de Paris, Grenoble, Clermont-Ferrand, Marseille et Toulouse sur 1070 enfants de 4 à 14 ans, asthmatiques ou témoins, recrutés en milieu hospitalier ; Considérant que l'étude consiste à recueillir, à partir de quatre questionnaires, des informations sur la santé respiratoire de l'enfant, les allergies de l'enfant et de la famille, des données sur l'habitat et l'environnement, l'histoire des lieux de séjour de l'enfant permettant de dégager l'index rétrospectif d'exposition au trafic automobile et le profil d'activité de chaque enfant en terme d'heures passées en différents lieux et environnements ; Considérant que chacun des questionnaires sera identifié par un numéro d'ordre, le nom de l'enfant étant conservé par chaque service pédiatrique hospitalier ; Considérant que les informations recueillies par le biais des questionnaires seront complétées par l'indication des mesures de la poussière, des aldéhydes et des oxydes d'azote au moyen de capteurs de la pollution dont seront dotés les enfants ;

Considérant que l'exploitation des données sera réalisée par chacun des services pédiatriques concernés ; que l'ensemble des données sera adressé avec le numéro d'ordre au laboratoire de santé publique de la faculté de médecine de Grenoble, chargé de l'analyse statistique des données ;

Considérant que les données ainsi recueillies sont pertinentes au regard de la finalité poursuivie ;

Prenant acte de ce que le Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, chargé d'apprécier la méthodologie de la recherche, l'utilité du recours aux données nominatives et la pertinence des données, a émis un avis favorable à la mise en œuvre du traitement ;

Considérant que les dispositions de l'article 40.5 de la loi du 6 janvier 1978 modifiée sont strictement respectées, chaque parent d'enfant étant informé par le médecin traitant hospitalier, au moyen d'une note individuelle, de la finalité de l'enquête, de l'identité des responsables et des modalités d'exercice du droit d'accès ; qu'en outre une copie de chacun des questionnaires leur sera remis et leur consentement recueilli sous forme expresse ;

Considérant que les sécurités mises en place pour garantir la confidentialité des données sont satisfaisantes ;

Autorise la mise en oeuvre par le laboratoire de santé publique de la faculté de médecine de Grenoble du traitement automatisé d'informations nominatives ayant pour finalité une étude épidémiologique sur l'asthme de l'enfant et les transports.

III. L'ACCES AU RNIPP POUR LES RECHERCHES EN SANTÉ

Dans la mesure où la réalisation d'études épidémiologiques repose sur un suivi de la santé dans le temps de groupes d'individus, les chercheurs ont souvent besoin de connaître les décès et les motifs du décès. Pour cela, ils adressent aux mairies de naissance une demande d'extrait d'acte de naissance des personnes dont ils fournissent l'identité et la date de naissance. En effet, aux termes du code civil, les mairies, dépositaires des registres d'état civil, sont tenues de délivrer des extraits d'acte de naissance à tout requérant. Une fois l'indication du décès obtenue, l'organisme de recherche doit recueillir la cause médicale de décès auprès du service commun n° 8 de l'INSERM, chargé de l'exploitation statistique nationale des certificats de décès.

Confrontés à cette procédure lourde et difficilement réalisable dès lors que l'échantillon de population concerné est important, et parfois sans réponse des mairies, les organismes de recherche ont souhaité pouvoir obtenir directement les informations relatives aux décès auprès du Répertoire national d'identification des personnes physiques (RNIPP) tenu par l'INSEE.

Saisie à ce sujet par le ministre du Travail et des Affaires sociales, la CNIL a donné un avis favorable à un projet de décret pris en application de l'article 18 de la loi du 6 janvier 1978, qui, d'une part autorise l'accès aux données relatives aux décès des personnes figurant au RNIPP dans le cadre des recherches et, d'autre part fixe les conditions dans lesquelles ces mêmes informations peuvent être communiquées respectivement par l'INSEE et par l'INSERM.

À cet égard, il convient de relever en premier lieu que seuls les organismes de recherche, publics ou privés, qui ont été autorisés par la CNIL au sens de l'article 40.2 de la loi du 6 janvier 1978 modifiée à mettre en oeuvre un traitement automatisé ayant pour fin la recherche dans le domaine de la santé, peuvent obtenir des indications de décès issues directement du RNIPP et ce, uniquement pour une recherche déterminée. Il ne s'agit donc, en aucune façon, d'une autorisation générale d'accès au RNIPP délivrée à tel ou tel organisme de recherche.

Par ailleurs, seules les données relatives à la date et au lieu de décès, assorties du numéro d'acte de décès, sont extraites du RNIPP, à partir d'une recherche effectuée par les nom et prénom, le sexe, la date et lieu de naissance des personnes concernées par la recherche ; mais en aucun cas, le numéro d'inscription au répertoire (NIR) ne peut être utilisé et communiqué.

Enfin, les données extraites suivent un circuit de transmission qui contribue à préserver la confidentialité. Ainsi, l'existence d'un intermédiaire, l'INSERM, entre l'organisme de recherche demandeur et l'INSEE, garantit que l'INSEE ne puisse pas connaître l'organisme demandeur, et disposer par exem-

ple d'indications sur les pathologies des personnes dont on cherche à connaître le statut vital.

Concrètement, une fois l'autorisation de la CNIL obtenue, l'organisme de recherche adresse au service de l'INSERM compétent, un fichier informatique comportant, pour chaque personne, le numéro d'identification individuel propre à l'étude et les nom, prénoms, sexe, date et lieu de naissance. Dans une seconde phase, l'INSERM transmet ce fichier, sans mention de l'organisme demandeur, à l'INSEE qui l'enrichit de la mention des dates et lieux de décès et des numéros d'acte de décès. En dernier lieu, l'INSEE restitue le fichier enrichi à l'INSERM, à charge pour ce dernier de supprimer les noms et prénoms, puis de transmettre le fichier ainsi expurgé au service commun n° 8 de l'INSERM, qui le complète de l'indication des causes de décès avant de le restituer à l'organisme demandeur.

Délibération n° 97-047 du 10 juin 1997 portant avis sur un projet de décret autorisant l'accès aux données relatives aux décès des personnes figurant au répertoire national d'identification des personnes physiques dans le cadre des recherches dans le domaine de la santé

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 l'article L. 363-1 du code général des collectivités territoriales ;

Vu le décret n° 78-778 du 17 juillet 1978 modifié pris pour son application ;

Vu le décret n° 82-103 du 22 janvier 1982 relatif au répertoire national d'identification de personnes physiques ;

Vu l'instruction générale de l'état civil du 21 septembre 1955 ;

Vu le projet de décret en Conseil d'État présenté par le ministre du Travail et des Affaires sociales ;

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

Après avoir entendu le représentant du ministre chargé de la gestion du répertoire ;

Considérant que le ministère du Travail et des Affaires sociales, conformément à l'article 18 de la loi du 6 janvier 1978, a saisi la Commission d'un projet de décret autorisant l'accès aux données relatives au décès des personnes figurant au répertoire national d'identification des personnes physiques, en vue d'effectuer des traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé ; Considérant que ce projet de décret définit également les conditions de communication de ces données ainsi que les modalités selon lesquelles les informations relatives aux causes de décès pourront être obtenues auprès du service commun n° 8 de l'INSERM, chargé, en application de l'article L.

363.1 du code général des collectivités territoriales de l'exploitation statistique nationale des certificats médicaux de décès ;

Considérant que seuls pourront utiliser le RNIPP les organismes, publics ou privés, qui auront été autorisés par la CNIL, conformément aux dispositions de l'article 40.2 de la loi du 6 janvier 1978 modifiée, à mettre en œuvre un traitement automatisé de données nominatives ayant pour fin une recherche dans le domaine de la santé ;

Considérant que les responsables de la recherche, au sein de ces organismes, ne pourront obtenir du RNIPP que les informations relatives aux date et lieu de naissances ainsi qu'au numéro d'acte de décès des personnes pour lesquels auront préalablement été communiqués l'identité, le sexe ainsi que les date et lieu de naissance ;

Prenant acte de ce que le numéro d'inscription au répertoire (NIR) ne sera pas utilisé ;

Considérant que des modalités spécifiques de circulation des données ont été prévues afin d'en garantir la confidentialité ;

Considérant ainsi que les organismes de recherche seront tenus d'adresser leur demande à un service particulier de l'INSERM qui se chargera de transmettre à l'INSEE, après occultation de l'identité de l'organisme demandeur, le fichier des personnes pour lesquelles l'organisme de recherche souhaite connaître le statut vital ;

Considérant que l'INSEE, après avoir complété ce fichier de l'indication des date et heure de décès, le restituera à l'INSERM ; que celui-ci, après suppression de l'identité des personnes le communiquera au service commun n° 8 de l'INSERM qui le complétera des informations relatives aux causes médicales de décès et le restituera à l'organisme demandeur ;

Considérant que ni l'INSEE ni l'INSERM ne conserveront copie des fichiers ainsi transmis ;

Émet un avis favorable au projet de décret présenté par le ministre du Travail et des Affaires sociales.

Chapitre 7

PROTECTION SOCIALE

I. LES PRÉALABLES À LA GÉNÉRALISATION DE « SESAM-VITALE »

En l'an 2000, chaque assuré et chaque professionnel de santé devrait être doté d'une carte électronique. L'assuré social devra présenter sa carte à son médecin et à son pharmacien pour pouvoir obtenir le remboursement de ses frais de consultation ou de ses médicaments sans avoir à envoyer sa feuille de soins à la caisse. Cette carte à puce comportera le numéro de sécurité sociale et les données socio-administratives nécessaires à sa prise en charge par la sécurité sociale, mais également dans une seconde phase, les informations médicales jugées utiles pour assurer une bonne continuité des soins entre les professionnels de santé qu'il sera amené à consulter. De leur côté, tous les médecins et pharmaciens pourront utiliser, grâce à leur propre carte, un réseau intranet pour télétransmettre aux organismes de sécurité sociale les feuilles de soins. Concrètement, le professionnel de santé devra tout d'abord introduire dans le lecteur connecté à son micro-ordinateur, sa carte d'identification professionnelle, puis la carte de l'assuré pour récupérer automatiquement l'identification de celui-ci, puis saisir le code détaillé de l'acte pratiqué, le cas échéant de la pathologie ou du médicament prescrit. La mise en œuvre de ce dispositif nécessite tout à la fois d'importants aménagements préliminaires des systèmes informatiques existants et la création d'applications nouvelles.

A. Les circuits d'informations générés par le RNIAM

Le répertoire national inter-régimes de l'assurance maladie (RNIAM) a été créé en 1996 pour recenser l'ensemble des 58 millions de personnes

bénéficiaires de l'assurance maladie, quel que soif leur régime, leur statut (ouvrant droit, conjoint, enfant) ou leur nationalité (les étrangers salariés bénéficiant de la sécurité sociale).

Actuellement en cours de constitution, ce fichier national est géré par la Caisse nationale d'assurance vieillesse (CNAVTS) qui assure déjà la gestion des procédures d'immatriculation à la sécurité sociale et la tenue, pour le compte de l'INSEE, de la section qui contient les données d'identification des personnes nées à l'étranger ou dans les TOM. Le RNIAM a vocation, d'une part à certifier l'identification et l'affiliation des personnes bénéficiaires de l'assurance maladie et, d'autre part à identifier les organismes d'assurance maladie dont relèvent les personnes.

Par délibération n° 96-070 du 10 septembre 1996, la CNIL s'est prononcée sur les modalités de fonctionnement du RNIAM, en tenant compte de l'ampleur du dispositif et de la centralisation, sur la base de l'identifiant national que constitue le numéro de sécurité sociale, d'informations permettant d'identifier avec certitude les personnes et même de les localiser grâce à l'indication de la caisse d'affiliation. C'est en ce sens que la Commission a notamment demandé que la liste des destinataires des informations issues de ce répertoire soit strictement limitée, et notamment que les caisses locales de sécurité sociale ne puissent pas y accéder directement (cf. 17^{e} rapport, p. 261).

En 1997, la nécessité d'accélérer la montée en charge du RNIAM a conduit à élaborer une réorganisation des circuits d'informations entre les services d'état civil des communes et du ministère des Affaires étrangères et l'INSEE d'une part, entre l'office des migrations internationales (OMI) et la CNAVTS d'autre part, et enfin, un fonctionnement modifié du RNIPP. Ces aménagements traduisent concrètement une utilisation du RNIPP par les communes et par le service central d'état civil du ministère des Affaires étrangères, ainsi qu'un transfert d'informations entre l'OMI et la CNAVTS.

Ces changements ont essentiellement trois objectifs :
- réduire les délais de transmission des actes d'état civil entre les communes et l'INSEE ;
- informatiser l'état civil des communes et du service central d'état civil du ministère des Affaires étrangères ;
- faciliter l'alimentation du RNIPP concernant les personnes entrant en France au titre du regroupement familial.

La CNIL a émis un avis favorable à un projet de décret en Conseil d'État relatif aux transmissions d'état civil à l'INSEE en vue de la tenue du RNIPP et un avis favorable à deux projets de décrets en Conseil d'État autorisant l'utilisation du RNIPP par les communes et le service central d'état civil du ministère des Affaires étrangères dans les traitements automatisés d'état civil. Cependant, ce dernier avis a été donné sous réserve que les textes réglementaires appelés à publication soient modifiés, de sorte qu'apparaisse clairement la nature exacte des données transmises par l'INSEE au service central d'état civil du ministère des Affaires étrangères et que l'INSEE ne transmet qu'aux communes que les

informations relatives aux personnes pour lesquelles elles ont compétences pour établir un acte de naissance ou de décès ; par ailleurs, il a été rappelé qu'en aucun cas, les registres d'état civil des mairies ne devront être corrigés au seul vu des données issues du RNIPP.

Délibération n° 97-068 du 23 septembre, 1997 portant avis sur un projet de décret en Conseil d'État relatif aux transmissions d'informations d'état civil à L'INSEE en vue de la tenue du RNIPP

(Déclaration de modification n° 7 916)

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, pris ensemble le décret n° 78-774 du 17 juillet 1978 ; Vu la loi n° 46-854 du 27 avril 1946 modifiée portant ouverture et annulation de crédits sur l'exercice 1946, notamment ses articles 32 et 33 ; Vu le code du travail, notamment l'article L. 341-9 ;

Vu le code de la sécurité sociale, notamment les articles R. 115-1 et 161-35, 36 et 38 ;

Vu le décret n° 82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques ;

Vu le décret n° 89-373 du 9 juin 1989 relatif aux modalités d'organisation de l'Institut national de la statistique et des études économiques ; Vu le projet de décret en Conseil d'État relatif aux transmissions d'informations d'état civil à l'INSEE en vue de la tenue du RNIPP ;

Après avoir entendu Messieurs Charles Renard et Maurice Viennois, 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 en Conseil d'État modifiant l'article 5 du décret n° 82-103 du 22 janvier 1982 et relatif aux transmissions d'informations d'état civil à l'INSEE en vue de la tenue du RNIPP ;

Considérant que le projet de décret soumis à la Commission a en premier lieu pour objet de préciser la nature et les délais de transmission des informations d'état civil devant être communiquées à l'INSEE par les services d'état civil des communes et le service central d'état civil du ministère des Affaires étrangères pour assurer la tenue du RNIPP ; qu'il est ainsi prévu que, lors de l'établissement de tout acte de naissance, les communes transmettent quotidiennement à l'INSEE les informations d'état civil recueillies, ce délai étant porté à un an pour les actes de naissance transmis par le service central d'état civil du ministère des Affaires étrangères, à un mois pour les informations recueillies lors de l'établissement des actes de mariage, de décès et de reconnaissance, à six mois pour les mêmes informations lorsqu'elles sont transmises par les agents consulaires français à l'étranger et faisant office d'officiers d'état civil, et à un an pour les mêmes

informations lorsqu'elles sont transmises par les officiers d'état civil de la collectivité territoriale de Saint-Pierre-et-Miquelon ;

Considérant que ces dispositions ont principalement pour objet de faciliter la tenue du répertoire national interrégime de l'assurance maladie qui a été institué par l'ordonnance du 24 avril 1996 sur la maîtrise médicalisée des dépenses de soins et dont les modalités de fonctionnement ont été fixées par un décret du 12 septembre 1996 et un arrêté du 22 octobre 1996 pris après avis favorable de la Commission ; que ce répertoire a notamment pour finalité de garantir la fiabilité des identifiants des bénéficiaires de l'assurance maladie, d'identifier avec certitude l'organisme qui leur sert les prestations d'assurance maladie et de contribuer aux procédures de délivrance et de mise à jour des cartes électroniques individuelles ; que ce répertoire sera alimenté par les données d'identification des ouvrants droit et des ayants droit dont disposent les organismes gérant les régimes de base d'assurance maladie ainsi que l'INSEE ;

Considérant que ces dispositions du projet de décret n'appellent pas d'observations particulières sur ce point ;

Considérant que le projet de décret prévoit en second lieu que les informations nécessaires à l'inscription dans la section « hors métropole » dite SHM du RNIPP pourront être issues des pièces justificatives présentées à l'Office des migrations internationales (OMI) par les ressortissants étrangers souhaitant entrer en France au titre des procédures de regroupement familial prévues par l'article 29 de l'ordonnance du 2 novembre 1945 modifiée ;

Considérant que ces informations doivent permettre à la CNAVTS, qui a reçu délégation de l'INSEE pour gérer la section hors métropole du RNIPP, d'assurer l'inscription au RNIPP de ces personnes ; que cette procédure de transmission d'informations est présentée comme devant permettre de faciliter la gestion des demandes d'immatriculation présentées ultérieurement par les organismes d'assurance maladie et de simplifier les démarches administratives des personnes concernées ; qu'enfin, elle dispenserait les agents des caisses d'avoir à contrôler la régularité des documents présentés par les personnes concernées par cette disposition ;

Considérant que dans la mesure où les informations transmises par l'OMI sont de même nature que celles que le ressortissant étranger est actuellement tenu de fournir aux caisses de sécurité sociale et où le dispositif mis en place doit contribuer à alléger les formalités mises à la charge de l'étranger avant qu'il puisse bénéficier des premiers remboursements de soins, cette transmission d'informations par l'OMI à la CNAVTS est légitime ;

Considérant que les dispositions du projet de décret sont appelées à être mises en oeuvre dès la publication de ce texte à l'exception de celles qui sont relatives aux délais de transmission des informations se rapportant aux actes établis par les officiers d'état civil communaux ; que ces dernières dispositions seront applicables le 1er janvier 1999 ; que toutefois les communes qui disposeraient avant cette date des moyens de transmettre par la voie informatique ou télématique ces informations à l'INSEE pourront, avant le 1er janvier 1999, respecter les nouveaux délais de transmission prévus par ce texte, sous réserve de l'accomplissement auprès de la CNIL par les communes concernées des formalités préalables à la mise en œuvre de telles transmissions automatisées ;

Considérant que le projet de décret renvoie à un arrêté le soin de fixer les conditions dans lesquelles l'INSEE versera aux communes une subvention forfaitaire destinée à faciliter les investissements nécessaires pour assurer sous forme télématique les transferts d'informations considérés ;

Émet un avis favorable au projet de décret en Conseil d'État relatif aux transmissions d'informations d'état civil à l'INSEE en vue de la tenue du RNIPP.

Délibération n° 97-069 du 23 septembre 1997 relative à deux projets de décret en Conseil d'État concernant l'autorisation d'utilisation du répertoire national d'identification des personnes physiques par les communes dans les traitements automatisés d'état civil et par le service central d'état civil du ministère des Affaires étrangères

(Déclaration de modification n° 7 916)

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 ;

Vu le décret n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres I^{er} à IV et VII de la loi n° 78-17 du 6 janvier 1978 ;

Vu le décret n° 46-1917 du 19 août 1946 modifié sur les attributions des agents diplomatiques et consulaires en matière d'état civil ;

Vu le décret n° 51 -284 du 3 mars 1951 relatif aux tables des registres d'état civil ;

Vu le décret n° 65-422 du 1er juin 1965 modifié portant création d'un service central d'état civil au ministère des Affaires étrangères ;

Vu le décret n° 80-308 du 25 avril 1980 modifié portant application des articles 98 à 98-4 et 99-1 du code civil relatifs à l'état civil des personnes nées à l'étranger qui acquièrent ou recouvrent la nationalité française et des articles 115 et 116 du code de la nationalité relatifs aux mentions intéressant la nationalité portées en marge des actes de naissance ;

Vu le décret n° 82-103 du 22 janvier 1982 modifié relatif au répertoire national d'identification des personnes physiques ;

Vu les deux projets de décret pris en application de l'article 18 de la loi du 6 janvier 1978 présentés par l'INSEE ;

Après avoir entendu Messieurs Charles Renard et Maurice Viennois, commissaires, en leur rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Considérant que l'INSEE a saisi la Commission de deux projets de décret relatifs à l'autorisation d'utilisation du répertoire national d'identification des personnes physiques (RNIPP) d'une part par les communes dans les traitements automatisés d'état civil, d'autre part par le service central d'état civil du ministère des Affaires étrangères ;

1) Sur l'autorisation d'utilisation du répertoire national d'identification des personnes physiques par les communes dans les traitements automatisés d'état civil.

Considérant qu'en application de l'article 18 de la loi du 6 janvier 1978, ce décret a pour objet d'autoriser les communes de métropole, des départements d'outre-mer et de la collectivité territoriale de Saint-Pierre-et-Mique-lon à utiliser le répertoire national d'identification des personnes physiques en vue de faciliter les recherches dans les tables d'état civil prévues par l'article 1 du décret du 3 mars 1951 ;

Considérant que ce projet vise à permettre aux communes de rapatrier, sur support informatique des informations d'état civil anciennes afin de reconstituer dans leur système informatique tout l'état civil de la commune ;

Considérant que les seules informations transmises par l'INSEE aux communes seront les nom, prénoms, sexe, date et lieu de naissance ou de décès, numéro d'acte de naissance ou de décès ;

Considérant que l'INSEE ne transmettra que les seules informations relatives aux personnes nées ou décédées dans la commune où sont établis l'un ou l'autre de ces actes ; qu'il y aura lieu de préciser le projet de décret sur ce point ;

Considérant qu'en aucun cas, le numéro d'inscription au répertoire (NIR) ne sera utilisé ;

Considérant que les données issues du répertoire n'ont pas la valeur authentique des actes d'état civil ; qu'elles constitueront simplement un équivalent des tables des registres mais sous une forme facilitant leur consultation ; que cette règle sera rappelée dans l'instruction générale relative à l'état civil en cours de mise à jour qui sera envoyée aux maires ;

Considérant que cette instruction générale devra rappeler qu'en cas de divergence entre les données issues du RNIPP et celles émanant de ses registres, la mairie ne sera pas habilitée à substituer les données obtenues du RNIPP à celles correspondantes de ses registres ; Considérant que cette utilisation du répertoire n'aura pas pour effet de porter à la connaissance des communes des informations qu'elles n'ont pas vocation à connaître et qu'elle est susceptible de contribuer à faciliter le fonctionnement des services d'état civil des communes ainsi qu'à améliorer les services rendus aux usagers puisque les réponses aux personnes qui demandent des copies ou des extraits d'actes seront facilitées ;

Considérant, en outre, que cette utilisation est de nature à assurer de manière constante le contrôle de la fiabilité des éléments contenus dans le répertoire, puisque toute absence de conformité des informations transmises par l'INSEE avec les tables de registres de l'état civil devra être portée à la connaissance de l'INSEE ; Considérant, dans ces conditions, que l'utilisation du répertoire est justifiée ;

2) Sur l'autorisation d'utilisation du répertoire national d'identification des personnes physiques par le service central d'état civil du ministère des Affaires étrangères (SCEC).

Considérant qu'en application de l'article 18 de la loi du 6 janvier 1978 ce décret a pour objet d'autoriser le service central d'état civil du ministère des Affaires étrangères à utiliser le répertoire national d'identification des personnes physiques en vue de faciliter les recherches dans les tables d'état

civil prévues à l'article 1er du décret du 3 mars 1951 dans le cadre des traitements automatisés qu'il met en œuvre ;

Considérant que les seules informations transmises par l'INSEE concerneront les nom, prénoms, sexe, date et lieu de naissance ou de décès, numéro de l'acte de naissance ou de décès concernant des personnes nées ou décédées à l'étranger ; qu'il y aura lieu de préciser le projet de décret sur ce point ; Considérant que le SCEC a vocation à centraliser la plupart des actes ou jugements relatifs à des événements d'état civil survenus à l'étranger concernant des Français ;

Considérant que cette utilisation devrait permettre d'accéder aux informations nominatives archivées dans le répertoire à l'exclusion du NIR, provenant des actes établis par ce service afin qu'il dispose d'un outil de recherche des actes, aussi performant que possible ;

Considérant que les données issues du répertoire n'ont pas la valeur authentique des actes d'état civil ; qu'elles constitueront simplement un équivalent des tables d'état civil mais sous une forme facilitant leur consultation ;

Considérant dans ces conditions, que cette utilisation, qui doit permettre d'améliorer le service rendu aux usagers et la qualité des registres du service central d'état civil, est justifiée ;

Émet :

— Un **avis favorable** au projet de décret relatif à l'autorisation d'utilisa tion du répertoire national d'identification des personnes physiques par les communes dans les traitements automatisés d'état civil sous la réserve suivante :
la fin du 1er alinéa de l'article 1er est rédigée comme suit : « Les informations concernant les nom, prénoms, sexe, date et lieu de naissance ou de décès, numéros d'actes de naissance ou de décès, pourront être transmises, à cet effet, par l'Institut national de la statistique et des études économiques aux communes qui ont établi l'un ou l'autre de ces actes ».

— Un **avis favorable** au projet de décret relatif à l'autorisation d'utilisa tion du répertoire national d'identification des personnes physiques par le service central d'état civil du ministère des Affaires étrangères, sous la réserve suivante : la fin du 1er alinéa de l'article 1er est rédigée comme suit : « Les informations concernant les nom, prénoms, sexe, dates et lieux de naissance ou de décès, numéros de l'acte de naissance ou de décès concernant des personnes nées ou décédées à l'étranger [...] ».

B. La poursuite des expérimentations des cartes à puce

L'expérimentation des cartes à puce « vitale », destinées à terme à tous les assurés sociaux, a débuté il y a une dizaine d'années (cf. 7e rapport, p. 199, 11e rapport, p. 274 et 14e rapport, p. 269). En 1997, la CNIL a été saisie par la Caisse nationale d'assurance maladie (CNAMTS) d'une ultime demande d'expérimentation du dispositif « SESAM VITALE ». Cette demande a visé, d'une part à prolonger les tests jusqu'en décembre 1997 et d'autre part, à supprimer le code porteur de la carte de l'assuré, qui constituait à l'origine une défense contre la fraude. La CNAMTS a en effet souligné que dans le cadre de l'expérimentation, la carte électronique ne revêtait pas un caractère proprement

individuel mais familial ; par ailleurs, la carte testée ne comporte aucun volet médical : elle est conçue de sorte que les informations ne soient accessibles que dans des conditions sécurisées, à savoir l'utilisation d'une carte de professionnel de santé (CPS) et d'un code porteur de professionnel de santé ou d'un agent de l'assurance maladie habilité, ce qui met à l'abri des risques d'atteinte à la confidentialité en cas de vol ou de perte.

Dans ces conditions, la Commission a émis un avis favorable au projet d'acte réglementaire modificatif présenté par la CNAMTS, tout en maintenant l'abandon ponctuel du code porteur ; pour autant, il a été rappelé que cela ne préjugeait en rien de l'avis qu'elle aura à rendre lorsqu'elle examinera la diffusion de la carte d'assuré social dotée d'un volet d'informations médicales.

Dans le même temps, la CNIL a également accepté la poursuite de l'expérimentation des cartes de professionnels de santé qui, à titre de rappel, comportent des fonctions d'identification des personnes et de sécurisation des télétransmissions (cf. délibération n° 96-064 du 9 juillet 1996, 17e rapport, p. 269).

Délibération n° 97-062 du 8 juillet 1997 portant avis sur le projet d'acte réglementaire modificatif présenté par la CNAMTS concernant la prolongation de l'expérimentation du dispositif « SESAM-VITALE »

(Demande d'avis modificative n° 103 860)

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 ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour son application ; Vu le code de la sécurité sociale ;

Vu l'ordonnance n° 96-346 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ;

Vu les délibérations n° 86-91 du 8 juillet 1986, n° 89-113 du 10 octobre 1989, n° 90-84 du 26 juin 1990 et n° 93-30 du 23 mars 1993 relatives au dispositif « SESAM-VITALE » ;

Vu le projet d'acte réglementaire modificatif présenté par la CNAMTS ;

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

Considérant que la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) a saisi la Commission d'une demande de modification du dispositif « SESAM-VITALE » tendant à l'autoriser à poursuivre, jusqu'au 31 décembre 1997, l'expérimentation de ce dispositif dans les circonscriptions des caisses primaires d'assurance maladie de Bayonne, Blois, Bou-logne-sur-Mer, Charleville-Mézières, Evreux, Lens et Rennes ;

Considérant que ce dispositif consiste à doter les assurés sociaux de cartes à microprocesseur (cartes VITALE) qui permettent aux professionnels de santé équipés de moyens informatiques et titulaires de cartes d'habilitation, de saisir les données nécessaires à la liquidation des prestations (feuilles de soins électroniques) et de les transmettre aux caisses concernées ;

Considérant que si l'ordonnance du 24 avril 1996 sur la maîtrise médicalisée des dépenses de soins, généralise d'ici à l'an 2000 les procédures de télétransmission des feuilles de soins électroniques et prévoit, l'attribution au 31 décembre 1998 à chaque assuré et au 1er janvier 2000 à chaque ayant droit, d'une carte électronique individuelle inter régimes destinée à remplacer la carte papier d'assuré social, l'entrée en application de ces dispositions est subordonnée à la parution de décrets, qui devront en particulier fixer le contenu et les modalités d'utilisation des cartes VITALE ;

Considérant, en outre, que les pouvoirs publics souhaitent assurer une montée en charge progressive du dispositif « SESAM-VITALE » ;

Considérant dès lors qu'il y a lieu d'autoriser la prolongation, jusqu'au 31 décembre 1997, de l'expérimentation du dispositif « SESAM-VITALE » ;

Considérant que la CNAMTS a également saisi la CNIL de deux modifications techniques relatives d'une part au remplacement, par des cartes de professionnels de santé (CPS), des cartes d'habilitation multi-services attribuées jusqu'à présent aux professionnels de santé relevant des sites d'expérimentation, et d'autre part à l'abandon du code secret dont est actuellement titulaire chaque assuré porteur d'une carte « VITALE » ; que la première modification envisagée ne soulève pas d'observation particulière ;

Prenant acte, en ce qui concerne l'abandon du code porteur, que dans le cadre de l'expérimentation, il est procédé à la diffusion de cartes « VITALE », non pas individuelles mais familiales ; que, dans la mesure où le code porteur est susceptible d'être communiqué par l'ouvrant droit aux ayants droit, la CNAMTS estime que la présence d'un code ne s'avère pas nécessaire ; qu'en outre, les informations socio-administratives qui sont enregistrées actuellement dans la carte « VITALE » et qui sont globalement identiques à celles figurant sur les cartes d'assuré ne sont accessibles qu'aux professionnels de santé et agents des caisses, titulaires de cartes d'habilitation et disposant de lecteurs ;

Considérant que, eu égard aux caractéristiques actuelles et au contenu socio-administratif de la carte « VITALE », il y a lieu d'admettre, dans le cadre de l'expérimentation, la demande de la CNAMTS relative à la suppression du code associé à la carte « VITALE » ;

Considérant cependant que cette position ne saurait préjuger de l'avis que rendra sur ce point la Commission lorsqu'elle sera saisie du dispositif relatif à la diffusion des cartes électroniques individuelles comportant un volet médical ; que la Commission devra être saisie en temps utile des modalités techniques envisagées pour assurer la sécurité et la confidentialité des données qui figureront sur ce volet médical ;

Émet, dans ces conditions, **un avis favorable** au projet d'acte réglementaire modificatif présenté par la CNAMTS.

Délibération n° 97-063 du 8 juillet 1997 relative a une demande d'avis modificative présentée par le groupement d'intérêt public de la carte de professionnel de santé (GIP-CPS) concernant un traitement automatisé d'informations nominatives ayant pour finalité l'émission, la distribution et la gestion des cartes de professionnel de santé « CPS »

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 ensemble le décret n° 78-774 du 17 juillet 1978, pris pour son application ;

Vu les articles 226-13 et 226-14 du nouveau code pénal ;

Vu l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ;

Vu l'arrêté du 28 janvier 1993 approuvant la Convention constitutive du groupement d'intérêt public de la carte de professionnel de santé ;

Vu la délibération n° 96-064 du 9 juillet 1996 concernant la mise en oeuvre, à titre expérimental, d'un traitement automatisé d'informations nominatives présenté par le GIP-CPS ayant pour finalité l'émission, la distribution et la gestion de cartes de professionnel de santé sur des sites de qualification terrain ;

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

Considérant que le groupement d'intérêt public de la carte de professionnel de santé — le GIP-CPS —, a saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis modificative qui a pour objet respectivement de prolonger, pour une durée d'un an l'expérimentation des cartes de professionnels de santé et d'étendre la diffusion et l'utilisation de cette carte aux sites d'expérimentation du dispositif SESAM-VITALE ;

Considérant que la CNIL a émis un avis favorable à la mise en œuvre de cette expérimentation par délibération n° 96-064 du 9 juillet 1996 ;

Considérant que cette carte, conforme aux spécifications techniques logicielles définies par le GIP-CPS a pour fonction d'identifier les professionnels de santé et de sécuriser les télétransmissions de la feuille de soins électronique ; qu'elle doit remplacer la CHMS (carte d'habilitation multi-services) actuellement utilisée sur les sites d'expérimentation SESAM-VITALE ;

Considérant que, une fois l'expérimentation terminée, la CNIL devra être saisie du projet de décret en Conseil d'État qui, conformément aux dispositions de l'ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins, définira le contenu, les modalités de délivrance et d'utilisation de la carte du professionnel de santé ;

Considérant que dans sa délibération n° 96-064 du 9 juillet 1996, la Commission avait demandé à être saisie du bilan de l'expérimentation avant le déploiement de la carte de professionnel de santé ;

Émet un avis favorable au projet d'acte réglementaire modificatif présenté par le GIP-CPS ;

Rappelle que la CNIL devra être informée du bilan de cette expérimentation avant sa généralisation.

C. La modernisation des procédures liées au remboursement des prestations

1) LE TRAITEMENT « PROGRÈS »

La CNIL a émis un avis favorable concernant un modèle type de traitement susceptible d'être mis en œuvre dans les caisses primaires d'assurance sociale, en remplacement du système « LASER » en vigueur depuis 1984, mais qui n'est plus assez performant pour répondre aux exigences imposées par l'ordonnance du 24 avril 1996 relative à la maîtrise des dépenses de soins — télétransmissions, feuilles de soins électroniques, cartes VITALE... — (cf. 17e rapport, p. 251).

En effet, cette nouvelle application dénommée « PROGRÈS », qui a pour finalité la saisie, le calcul et le paiement des prestations d'assurance maladie, multiplie les possibilités d'accès aux dossiers, sur la base de l'immatriculation fournie par le répertoire national d'identification de l'assurance maladie (RNIAM) ; de plus, chaque poste de travail d'une caisse peut accéder à la totalité des dossiers des assurés gérés par la caisse, et effectuer, en temps réel, la totalité des tâches inhérentes à la gestion des remboursements. Par ailleurs, « PROGRÈS » intègre un important système d'aide à la décision, sans pour autant requérir l'enregistrement de nouvelles informations. La durée de conservation a été réduite de 5 à 3 ans, dans la mesure où les demandes de remboursement se prescrivent après deux ans et trois mois.

La sécurité du traitement est assurée par un logiciel qui contrôle l'accès aux postes de travail grâce à des cartes à puce délivrées aux agents des caisses ; un système d'habilitation gère ensuite les applications qui leur sont accessibles ; enfin, une procédure de journalisation des connexions en permet un contrôle a *posteriori.*

Afin d'assurer une meilleure information des assurés sur les droits qui leurs sont reconnus par la loi du 6 janvier 1978, la CNIL a préconisé que les mesures de publication et d'affichage prévues soient complétées par un message porté directement sur les décomptes de prestations.

Délibération n° 97-002 du 14 janvier 1997 portant avis sur un projet d'acte réglementaire présenté par la caisse nationale d'assurance maladie des travailleurs salariés relatif à un modèle type de traitement automatisé d'informations nominatives dénommé « PROGRES » ayant pour finalité d'assurer le remboursement des prestations

(Demande d'avis n° 435 217)

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, pris pour son application ;

Vu l'ordonnance n° 67-706 du 21 août 1967 relative à l'organisation administrative de la sécurité sociale, ainsi que le décret d'application n° 67-1232 du 22 décembre 1967 modifié par le décret n° 69-14 du 6 janvier 1969 ;

Vu la loi n° 93-8 du 4 janvier 1993 relative aux relations entre les professions de santé et l'assurance maladie, au codage des actes et des prestations remboursables par l'assurance maladie ainsi que le décret n° 95-564 du 6 mai 1995 ;

Vu l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ;

Vu le décret n° 96-793 du 12 septembre 1996 autorisant les organismes de la branche maladie du régime général de la sécurité sociale à faire usage du numéro d'inscription au répertoire national d'identification des personnes physiques ;

Vu le code de la sécurité sociale ;

Vu l'avis favorable de la CNIL en date du 26 juillet 1984 sur le traitement « LASER » ;

Vu les délibérations n° 95-161 du 17 décembre 1995 et n° 96-050 du 4 juin 1996 relatives à l'intégration dans le traitement de gestion des caisses du codage des actes de biologie et des médicaments ;

Vu le projet d'acte réglementaire présenté par la caisse nationale d'assurance maladie des travailleurs salariés ;

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

Considérant que la caisse nationale d'assurance maladie des travailleurs salariés a saisi la Commission d'une demande d'avis relative à un modèle-type de traitement automatisé d'informations nominatives dénommé « PROGRES » ayant pour finalité la saisie, le calcul et le paiement des prestations d'assurance maladie ;

Considérant que ce traitement a vocation à se substituer au système « LASER » (Liquidation assistée sur équipement réparti) actuellement en vigueur dans les caisses ;

Considérant que si la finalité du traitement « PROGRES » demeure inchangée par rapport à l'application « LASER », cette application comporte des fonctionnalités nouvelles et repose sur l'utilisation de moyens informatiques et de logiciels plus performants, permettant tout à la fois d'améliorer et d'accélérer les procédures de liquidation et d'optimiser le service rendu aux assurés ;

Considérant que « PROGRES » a été conçu de façon à privilégier l'approche individuelle des dossiers ; qu'en conséquence, l'accès aux informations sera désormais possible non plus seulement par l'indication de l'identité de l'ouvrant droit mais par celle de tout assuré, qu'il soit ouvrant ou ayant droit ;

Considérant que l'application sera mise en oeuvre sur des postes de travail multifonctions — micro-ordinateurs et non plus terminaux passifs comme dans le cas de « LASER » — permettant aux agents d'effectuer, en temps réel, la totalité des traitements relatifs au remboursement des prestations en nature, d'hospitalisation, prestations diverses (prestations supplémentaires, capital décès, régularisations, recours tiers, forfaits...) et d'aboutir au décompte final ;

Considérant que cette application permettra également d'effectuer des contrôles sur l'ensemble des dossiers traités, quel que soit le mode de saisie des informations y figurant, qui seront systématiques, par sondage ou sélectifs ;

Considérant que les informations enregistrées dans le traitement, habituellement utilisées pour la liquidation des prestations portent notamment sur le NIR, l'identification des assurés, les modalités de prise en charge et de remboursement des prestations ainsi que la nature des actes et des prestations ; que ces informations sont adéquates, pertinentes et non excessives au regard de la finalité du traitement ;

Considérant que la durée de conservation des informations sur support informatique est de trois ans excepté lorsque celles-ci sont l'objet d'un litige ; que dans ce cas, ces informations sont conservées jusqu'à la clôture de celui-ci ;

Considérant que le traitement sera mis en oeuvre sur des micro-ordinateurs installés dans chaque centre de paiement et reliés à des serveurs locaux communiquant avec les centres de traitements informatiques gérant les bases de données et les applications centrales de production ;

Considérant que la sécurité et la confidentialité des informations traitées est assurée par la présence d'un logiciel dénommé « ARAMIS » qui permet de contrôler l'accès aux postes de travail grâce à des cartes à puce délivrées aux agents ;

Considérant par ailleurs qu'un système d'habilitation permet aux agents de n'accéder qu'aux applications qui leur ont été autorisées ;

Considérant enfin qu'une journalisation de toutes les transactions et événements sera effectuée, que ce soit au niveau du poste de travail ou au niveau du serveur ;

Considérant que le droit d'opposition mentionné à l'article 26 de la loi du 6 janvier 1978 ne s'applique pas à ce traitement ;

Considérant qu'il convient que les assurés soient informés des droits qui leur sont reconnus par la loi du 6 janvier 1978 par une mention figurant sur les décomptes de prestations ;

Considérant qu'une plaquette d'information doit être distribuée au personnel des caisses utilisant le système « PROGRES » à l'occasion de la mise en place du système « ARAMIS », plaquette spécifiant les caractéristiques de ce serveur et notamment la mise en place d'un audit des connexions de chaque agent ;

Considérant que chaque caisse adoptant le système présenté par ce modèle-type devra adresser à la CNIL une déclaration simplifiée comportant un engagement de conformité et une proposition de rédaction d'un message destiné à informer les assurés des droits qui leurs sont reconnus par la loi du 6 janvier 1978 qui pourra, le cas échéant, figurer sur les décomptes de prestations ;

Émet un avis favorable au projet d'acte réglementaire présenté par la CNAMTS.

2) LES FEUILLES DE SOINS ÉLECTRONIQUES

La généralisation des procédures de télétransmission des feuilles de soins constitue l'un des volets de la réforme du système de santé lancée en 1996. L'informatisation des feuilles de soins et de leur traitement répond à un souci de simplification et de modernisation des procédures de remboursement, allié à une volonté de maîtrise des dépenses, cette procédure devant fournir aux caisses des informations détaillées sur les comportements des assurés et les pratiques des professionnels de santé. Aussi, conformément à l'ordonnance du 24 avril 1996, un projet de décret en Conseil d'Etat précisant le contenu des feuilles de soins et des ordonnances électroniques, ainsi que les modalités de télétransmission de ces documents aux caisses de sécurité sociale, a été élaboré par le ministère de l'Emploi et de la Solidarité qui l'a soumis pour avis à la CNIL.

Jusqu'à présent, hormis les procédures de fiers payant, c'est l'assuré qui règle lui-même son médecin et son pharmacien, avant d'être remboursé par sa caisse d'assurance maladie de rattachement au vu de l'original de la feuille de soins papier établie par le praticien, qui indique la nature et le tarif de l'acte pratiqué selon la nomenclature en vigueur. L'assuré quant à lui doit la remplir, puis l'adresser au centre de paiement de son organisme d'assurance maladie qui saisit dans ses traitements les informations portées sur cette feuille et procède au remboursement total ou partiel des frais exposés par l'assuré. Or le dispositif qui ressort du projet de décret présenté à la CNIL bouleverse radicalement ces pratiques, dans la mesure où les professionnels de santé sont conduits à assurer eux-mêmes la télétransmission des feuilles de soins, tandis que les assurés sont déchargés de toute démarche administrative vis-à-vis des caisses.

S'agissant des informations ayant vocation à figurer sur les nouvelles feuilles de soins et les ordonnances, le projet de décret énumère les grandes catégories et indique qu'un arrêté pris ultérieurement en précisera le contenu détaillé. Sur ce point, la Commission a considéré que le projet de décret devrait être complété d'une mention indiquant que l'arrêté sera pris après avis de la CNIL. Par ailleurs, il est fait état d'une rubrique exhaustive destinée à recenser « les informations nécessaires au remboursement des prestations » (identification

de l'assuré et du professionnel et renseignements sur l'acte ou la prestation) et d'une rubrique relative aux « informations utiles à la santé publique ou à la maîtrise des dépenses de santé » ; il s'agit essentiellement d'indications permettant, à des fins de contrôle, de rapprocher aisément les feuilles de soins des ordonnances. En l'absence de précisions sur la nature exacte des données susceptibles d'être enregistrées dans cette rubrique, la CNIL a demandé que soit supprimée dans cette rubrique la référence faite à la santé publique.

S'agissant des droits des personnes, la CNIL a estimé que la suppression de la délivrance d'une feuille de soins au profit d'un système qui décharge l'assuré de toute démarche, ne doit pas conduire à le priver de la possibilité de connaître les informations le concernant et qui sont transmises aux organismes de sécurité sociale. Dès lors, la Commission a proposé une modification du projet de décret qui permette à l'assuré qui en fait la demande d'obtenir un duplicata de la feuille de soins transmise par voie électronique.

Enfin, dans un souci d'allégement des formalités préalables, les caisses devant modifier leurs traitements ont été dispensées d'avoir à déposer une demande d'avis modificative auprès de la CNIL.

Délibération n° 97-070 concernant un projet decret relatif aux documents conditionnant le remboursement des prestations en nature des assurances maladie, maternité et accidents du travail et contribuant à la maîtrise des dépenses de santé présenté par le ministère de l'Emploi et de la Solidarité

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, ensemble le décret n° 78-774 du 17 juillet 1978, 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 et, notamment, ses articles L. 161-29, L. 161-31, L. 161-34, L. 162-4, L. 161-12-5, L. 174-4, L. 322-3 et L. 371-6;

Vu le code rural ;

Vu le code de la santé publique et, notamment, ses articles L. 625, L. 666-9 et L. 710-16-2

Vu le projet de décret en Conseil d'Etat 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 le ministère de l'Emploi et de la Solidarité a saisi la Commission d'un projet de décret relatif aux documents conditionnant le remboursement des prestations en nature des assurances maladie, maternité et accidents du travail et contribuant à la maîtrise des dépenses de santé ;

Considérant qu'aux termes de l'article L. 161-33 du code de la sécurité sociale, issu de l'ordonnance du 24 avril 1996, « l'ouverture du droit aux prestations de l'assurance maladie est subordonnée à la production de documents dont le contenu, le support ainsi que les conditions et délais de transmission à la caisse du bénéficiaire sont fixés par décret en Conseil d'État » ; Considérant que le projet de décret soumis à la CNIL a pour objet de préciser le contenu des feuilles de soins et des ordonnances ainsi que les nouvelles modalités de transmission de ces documents aux caisses de sécurité sociale ; Considérant que le dispositif prévu poursuit un objectif de simplification et de modernisation des formalités de remboursement et tend à harmoniser les textes relatifs aux procédures de demandes de remboursements pour l'ensemble des régimes qui sont actuellement dispersés dans le code de la sécurité sociale et celui de la santé publique ; qu'à cet effet, le décret :

- prévoit la possibilité de transmettre les feuilles de soins conditionnant le remboursement des prestations en nature pour les risques maladie, maternité et accidents du travail par voie électronique sans envoi parallèle des documents papier ;
- énumère les catégories d'informations nécessaires au remboursement de l'assuré ainsi que les catégories d'informations supplémentaires utiles à la santé publique ou à la maîtrise des dépenses de santé (article R. 161-33-1, article R. 161-33-2) ;
- précise que les spécifications (pour les documents électroniques) et les modèles (pour les documents papier) des feuilles de soins et des ordonnances sont fixés par un arrêté conjoint des ministres chargés de la Sécurité sociale, de l'Agriculture, du Budget et de la Santé (article R. 161-33 et R. 161-33-3) ;
- précise les conditions et les délais de transmission des feuilles de soins et des ordonnances aux caisses locales et détermine le responsable des transmis sions dans les différentes hypothèses (transmission électronique, utilisation d'un support papier avec paiement direct ou en cas de tiers-payant) de même que les sanctions applicables dans chaque cas (article R. 161-33-5) ;
- exonère les professionnels de santé de l'obligation de produire une note ou une facture lorsque le patient règle par chèque ou par carte bancaire et prévoit la délivrance d'une facture lorsque ce dernier règle en espèces (article R. 161-33-6).

Sur l'article R. 161-33

Considérant que cette disposition renvoie à un arrêté le soin de préciser le contenu détaillé des feuilles de soins et des ordonnances ;

Considérant que cet article devrait être complété de façon à préciser que la CNIL devra être saisie du projet d'arrêté ;

Sur l'article R. 161-33-2

Considérant que cet article précise, en son premier alinéa, « les catégories d'informations supplémentaires utiles à la santé publique ou à la maîtrise des dépenses de santé » ;

Considérant cependant que les informations sont essentiellement des indications qui, portées tout à la fois sur les feuilles de soins et les ordonnances, ont pour objet de permettre aux services de contrôle des caisses de rapprocher sans difficulté ces différents documents ; que ces informations contribuent uniquement à la maîtrise des dépenses de santé ;

Considérant, en conséquence, que la référence faite à la santé publique pourrait être supprimée dans le premier alinéa ;

Sur l'article R. 161-33-6

Considérant qu'il résulte de cet article, qu'en cas de transmission de la feuille de soins par voie électronique, l'assuré ne disposera pas de justificatif de l'acte effectué par son praticien mais uniquement, et dans la seule hypothèse où il réglera le praticien au moyen d'espèces, d'un reçu de paiement ;

Considérant dès lors que l'assuré ne sera plus en mesure de vérifier, comme il peut le faire actuellement en lisant la feuille de soins qui lui est remise, la nature des informations qui seront transmises à sa caisse, et, tout particulièrement celles relatives à la consultation qu'il a subie ; qu'en tout état de cause, le reçu, qui n'est d'ailleurs remis qu'au patient ayant réglé en espèces, ne saurait lui apporter des informations aussi complètes que celles qui figurent sur la feuille de soins ;

Considérant qu'il est légitime que le patient qui le souhaite puisse disposer des informations le concernant qui sont transmises à sa caisse ;

Considérant que l'article 2 du projet de décret devrait être complété par un article R. 161-33-7 nouveau ainsi rédigé : « un duplicata de la feuille de soins transmise par voie électronique est remis, sur sa demande, à l'assuré par le professionnel de santé » ;

Sur les formalités préalables à accomplir auprès de la CNIL par les caisses

Considérant que le projet de décret aura pour effet de modifier ou compléter les informations dont disposent les caisses dans leurs traitements automatisés d'informations nominatives tant à l'égard des assurés que des professionnels de santé ; qu'ainsi, les demandes d'avis initialement présentées par les caisses et ayant recueilli un avis favorable de la CNIL en application de l'article 15 de la loi du 6 janvier 1978 devraient être modifiées, en application de cette même procédure ; que dans le souci de dispenser les caisses d'avoir à accomplir une telle formalité administrative, alors que les modifications soumises à l'avis de la CNIL se limiteraient à tirer les conséquences du dispositif nouveau prévu par le présent projet de décret et par le futur arrêté auquel le présent projet de décret renvoie, ces deux derniers textes ayant été pris après avis de la CNIL, il y a lieu de proposer que le projet de décret soit complété par un article nouveau ainsi rédigé :

« Les organismes chargés de la gestion d'un régime obligatoire de base de la sécurité sociale sont dispensés, par dérogation à l'article 12 du décret n° 78-774 du 17 juillet 1978 pris pour l'application de la loi n° 78-17 du 6 janvier 1978, de présenter à la Commission nationale de l'informatique et des libertés, une demande d'avis modificative accompagnée d'un projet d'acte réglementaire prévue par l'article 15 de ladite loi, lorsque cette demande d'avis n'a d'autre objet que de modifier ou compléter, en application des dispositions du présent décret, les catégories d'informations nominatives enregistrées dans leurs traitements » ;

Est d'avis que le projet de décret devrait être modifié dans le sens des observations qui précèdent.

II. L'EDITION DES DECOMPTES À LA CPAM DE HAGUENAU

La Caisse primaire d'assurance maladie de Haguenau a saisi la Commission d'une nouvelle demande d'avis relative à la mise en place dans des banques, de bornes d'information et d'édition des décomptes de prestations de sécurité sociale, à l'intention des assurés sociaux, clients de ces établissements. L'intérêt essentiel de ce dispositif est de donner la possibilité aux assurés de connaître au jour le jour le détail des virements effectués sur leurs comptes, sans subir les inconvénients liés au regroupement des décomptes, instauré par les caisses pour réduire leurs coûts de gestion. En effet, si le paiement des prestations s'effectue quotidiennement, les CPAM, dans un souci de rationalisation des dépenses, regroupent l'édition des décomptes sur une durée variant en général de quinze jours à un mois.

En 1995, un projet de même nature avait donné lieu à un avis défavorable de la CNIL du fait qu'une seule banque fut-elle fortement implantée dans la région, était concernée par le partenariat avec la CPAM de Haguenau. La Commission avait en effet estimé que, en l'état, le traitement aboutirait à ce qu'un organisme détenant des informations au titre d'une mission de service public, ne soit pas en mesure d'offrir les mêmes services à tous les assurés (cf. 16^{e} rapport, p. 319).

En 1997, un nouveau projet revu à la lumière de la délibération de la CNIL n° 95-100 du 11 juillet 1995, associait trois organismes bancaires représentant à eux seuls 80 % des virements de la CPAM, une proposition de partenariat ayant par ailleurs été adressée à l'ensemble de la profession.

Techniquement, il est prévu que le centre informatique de la caisse procède à l'extraction des informations relatives à la liquidation des prestations concernant les assurés titulaires d'un compte dans l'une des trois banques concernées, et ce, à partir du seul critère de l'identité bancaire. À une date butoir se situant trente jours maximum après la date de transmission d'un fichier contenant ces données vers les banques prestataires, les informations ayant donné lieu à édition sur borne sont automatiquement supprimées du fichier, tandis que celles qui n'ont pas été sollicitées sont renvoyées vers le centre informatique afin de les faire parvenir aux assurés selon la procédure habituelle. Au surplus, il a bien été précisé qu'en aucun cas les banques ne pourraient enregistrer ou consulter les informations transmises par la CPAM dans le cadre de cette application ; il importe en effet que la confidentialité des données relatives aux actes médicaux ou aux prestations soit parfaitement garantie.

Comparé à l'application « Télématique grand Public » de la CNAMTS qui a aussi vocation à informer, grâce à des bornes situées dans des lieux publics, de la date de la liquidation des prestations, le système proposé par la caisse de Haguenau présente l'avantage de rendre compte de la date de virement sur le compte des prestations, donc de la disponibilité réelle de l'argent

(cf. 17e rapport, p. 286). Consultée sur le projet, la CNAMTS a d'ailleurs indiqué que le dispositif de la CPAM de Haguenau présentait de ce point de vue un intérêt incontestable. La CNIL a été de surcroît très sensible au fait que les assurés clients d'une banque, mais ne disposant pas d'une carte bancaire, pourront obtenir gratuitement une carte de libre service bancaire, afin de profiter des bornes d'information.

Enfin, la CPAM a prévu, en plus d'une campagne locale d'information, de recueillir le consentement exprès des personnes concernées au moyen d'une lettre d'adhésion qui leur serait adressée préalablement à l'implantation des bornes d'information, et de porter sur le décompte de prestations un message offrant aux assurés la possibilité de renoncer à tout moment à bénéficier de ce service.

Dans ces conditions, et notamment au regard du service rendu aux assurés, en particulier ceux qui disposent de faibles revenus, la CNIL a émis un avis favorable au traitement présenté par la CPAM d'Haguenau.

Délibération n° 97-078 du 21 octobre 1997 relative à la demande d'avis de la caisse primaire d'assurance maladie de Haguenau concernant l'édition de décompte de prestations de sécurité sociale sur imprimante libre service
(Demande d'avis n° 528 645)

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, pris pour son application.

Vu le projet d'acte réglementaire présenté par la CPAM de Haguenau ;

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

Considérant que la caisse primaire d'assurance maladie de Haguenau a saisi la Commission d'une demande d'avis relative à un traitement automatisé d'informations nominatives concernant un système d'édition de relevés de prestations d'assurance maladie sur imprimantes libre service (ILS) ;

Considérant qu'il s'agit pour la CPAM de permettre aux assurés sociaux disposant d'une carte bancaire délivrée, à titre gratuit ou onéreux, par l'établissement dont ils sont clients de pouvoir obtenir, par l'intermédiaire de bornes appelées ILS implantées aux emplacements des guichets automatiques de banque, l'édition du décompte des prestations de sécurité sociale qui ont été liquidées et virées sur leur compte bancaire ;

Considérant que le traitement projeté par la CPAM de Haguenau permettrait d'éviter les inconvénients liés au regroupement des décomptes sur une durée variant en général de quinze jours à un mois en permettant à l'assuré de

connaître, au jour le jour, le détail des prestations dont son compte bancaire vient d'être crédité ;

Considérant, en outre, que la mise en oeuvre de l'édition sur ILS dispensera la CPAM d'adresser par voie postale les décomptes aux assurés qui auront utilisé ce procédé ; qu'ainsi, la mise en oeuvre de ce système permettrait à la caisse de réaliser des économies de gestion ;

Considérant que la CPAM d'Haguenau a proposé à l'ensemble des établissements bancaires implantés dans sa circonscription de la caisse un partenariat destiné à offrir à l'ensemble des assurés le service proposé ; que le Crédit mutuel, la caisse d'épargne et la Banque populaire, qui sont destinataires à eux trois de 80 % des virements opérés, ont, seuls à ce jour, accepté ce partenariat ;

Considérant que le centre de traitement informatique des CPAM (CTI/AM) procédera à l'extraction d'informations relatives à la liquidation des prestations concernant uniquement les assurés titulaires d'un compte dans l'une des trois banques concernées ; que le critère de sélection utilisé sera l'identité bancaire et non le NIR ;

Considérant que ces informations seront transmises aux prestataires de service des trois établissements bancaires concernés qui les mettront à la disposition des assurés au moyen des guichets automatiques (ILS) ;

Considérant que l'exploitation de ces informations par les prestataires de service informatique des banques sera limitée à des opérations purement techniques et portera sur des données qui ne pourront être conservées que pendant une durée de trente jours maximum ; qu'en outre, l'application d'édition automatique sera en tous points distincte de la gestion du compte bancaire, les informations relatives aux rubriques d'actes et prestations remboursés n'étant en aucune façon enregistrées ou consultables par la banque ;

Considérant que les informations ayant donné lieu à édition sur borne ILS seront automatiquement supprimées du fichier dès l'édition réalisée et, qu'à une date butoir se situant trente jours maximum après la date de transmission de l'exemplaire du fichier vers les prestataires, les informations n'ayant pas donné lieu à consultation seront renvoyées vers le CTI ; que les assurés qui n'auront pas sollicité l'édition de leurs décomptes sur l'**ILS** les recevront selon la procédure et dans les délais habituels ;

Considérant qu'une convention est passée entre la CPAM et chaque prestataire de services par laquelle ce dernier s'engage à respecter l'ensemble des conditions précitées ;

Considérant que la CPAM prévoit que la population concernée sera préalablement informée de la mise en œuvre du traitement par une campagne dans la presse locale et dans le journal de l'assurance maladie de l'Alsace du Nord ainsi que par la diffusion d'une plaquette de présentation ;

Considérant que la CPAM a également prévu de recueillir le consentement exprès des personnes concernées au moyen d'une lettre d'adhésion qui leur serait adressée préalablement à la mise en oeuvre de la procédure ; que cette lettre devra également mentionner la possibilité, pour les assurés, de renoncer à tout moment à cette procédure ; qu'en outre, un message figurant sur le décompte des prestations informera également les assurés de cette possibilité ;

Considérant que dans la mesure où la CPAM est disposée à offrir le service à tous les assurés titulaires d'un compte en banque même si, à ce jour, seuls trois établissements bancaires ont accepté ce partenariat, il y a lieu de souligner l'intérêt que revêt ce dispositif pour 80 % des assurés ; qu'en effet, la connaissance de la date du virement sur le compte bancaire et donc la certitude d'une liquidité disponible présente un intérêt non négligeable pour les assurés et notamment ceux qui disposent de faibles revenus ;

Considérant qu'au regard des garanties de protection des données personnelles prévues par la CPAM, aucune disposition de la loi du 6 janvier 1978 ne s'oppose à la mise en œuvre de cette procédure ; **Émet dans ces conditions** un avis favorable au projet d'acte réglementaire présenté par la CPAM de Haguenau.

III. LE REGIME SPECIFIQUE DES ARTISTES PLASTICIENS ET GRAPHISTES

Les artistes auteurs d'œuvres graphiques et plastiques bénéficient d'un régime de protection sociale spécifique dont la charge a été confiée à la « Maison des artistes ». Créée pour agir en faveur des artistes des arts graphiques et plastiques, cette association (6000 membres), s'est vu attribuer des missions de sécurité sociale obligatoire. À ce titre, la « Maison des artistes » assure le recouvrement des cotisations et des contributions dues par les artistes (12 000 recensés), et se charge de leur affiliation, en particulier de la détermination de leur qualité d'artiste professionnel, mais en revanche, ne leur verse pas de prestations.

Dans ce contexte de double mission impartie à la « Maison des artistes », le Syndicat national des créateurs en arts graphiques et plastiques Force ouvrière a saisi la Commission d'une plainte relative aux conditions d'utilisation du fichier de gestion du régime de sécurité sociale des artistes auteurs d'oeuvres graphiques et plastiques. Le syndicat reproche à l'association de se servir de ce fichier pour adresser des informations sans relation directe avec cette mission de service public. Les requérants contestent en outre l'envoi, par la Maison des artistes, d'une lettre d'information mensuelle contenant par exemple un encart publicitaire pour une institution privée de prévoyance, ou encore un appel de caractère politico-syndical à une manifestation.

Par délibération n° 97-029 du 22 avril 1997, la CNIL a décidé de procéder à une mission de vérification sur place auprès de cette association pour examiner les modalités de fonctionnement du fichier de gestion des membres de la Maison des artistes au regard de la loi du 6 janvier 1978. Cette mission, qui a été effectuée en deux temps, les 14 mai et 11 juin 1997, a permis de révéler que, jusqu'à une période récente, il n'y avait effectivement pas de réelle dissociation entre les deux activités de l'organisme en cause, et qu'un seul fichier était utilisé pour gérer les membres adhérents de l'association et les

artistes affiliés au régime de sécurité sociale. Or, c'est précisément cette situation qui avait conduit à ce que les assurés, y compris ceux qui ne sont pas adhérents de la Maison des artistes, aient reçu des informations de toute nature, notamment commerciales ou politiques.

Il a été indiqué à la Commission que, désormais, le fichier des artistes affiliés à la sécurité sociale était parfaitement distinct du registre manuel des membres de l'association. En conséquence, la CNIL a rappelé à cet organisme la nécessité de respecter le principe de finalité selon lequel, au risque d'encourir des sanctions pénales, des informations ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été recueillies. Par ailleurs, la Commission a estimé utile d'appeler l'attention du ministère de l'Emploi et de la Solidarité sur ce dossier.

Délibération n° 97-095 du 2 décembre 1997 relative aux vérifications sur place effectuées le 14 mai et le 11 juin 1997 auprès de la Maison des artistes

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 pris pour l'application de la loi susvisée ;

Vu le code de la sécurité sociale ;

Vu la délibération n° 97-029 du 22 avril 1997 ;

Vu la délibération n° 97-043 du 27 mai 1997 ;

Vu les comptes rendus des missions de vérification sur place effectuées le 14 mai et le 11 juin 1997;

Vu la lettre du 25 novembre 1997 du président de la Maison des artistes ; Vu le règlement intérieur de la Commission et, notamment, son article 54 ;

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

Considérant que la Maison des artistes, association loi de 1901 agréée pour assurer notamment les obligations de l'employeur en matière d'affiliation des artistes auteurs d'oeuvres originales graphiques et plastiques et le recouvrement des cotisations et contributions, a fait l'objet d'une plainte du syndicat national des créateurs en arts graphiques et plastiques Force ouvrière (SNCAGP-FO) au motif qu'elle aurait utilisé le fichier des assurés sociaux pour adresser des informations sans relation directe avec la mission de service public qui lui est dévolue par l'article L. 382-4 du code de la sécurité sociale ;

Considérant que les artistes plasticiens assurés sociaux, y compris ceux qui ne sont pas adhérents de la Maison des artistes, ont ainsi reçu pendant des années une carte leur permettant notamment de bénéficier de la gratuité d'accès aux musées nationaux ainsi que la « Lettre de la Maison des

artistes », document d'information à caractère politico-syndical émanant de l'association ;

Considérant qu'un courrier du président de la CNIL ainsi que plusieurs interventions du ministère des Affaires sociales auprès de la Maison des artistes ont eu pour effet d'interrompre, depuis 1995, la diffusion de cette lettre auprès des artistes non adhérents à l'association ; Considérant que la Commission a estimé nécessaire de procéder à deux missions de vérification sur place auprès de la Maison des artistes afin de contrôler les modalités de fonctionnement tant du fichier de gestion des membres de l'association que du fichier des assurés ; que ces missions ont eu lieu le 14 mai et le 11 juin 1997 ;

Considérant qu'il a été constaté que la Maison des artistes, organisme de sécurité sociale, dispose de deux fichiers informatisés qui concernent respectivement les artistes et les diffuseurs qui tiennent un rôle d'employeur ; Considérant que selon le vice-président de la Maison des artistes, cette dernière, au titre de ses activités associatives, constitue son propre fichier de membres qui n'est pas informatisé ; que les coordonnées des artistes qui se manifestent auprès de l'association sont notées, par ordre alphabétique, sur un registre manuel ; que les adresses des membres sont reproduites de façon manuscrite sur les enveloppes de correspondance et qu'aucun moyen informatique n'est utilisé pour l'envoi de ces documents ; Considérant qu'il n'a pas été matériellement possible de consulter ce registre manuel lors de la mission de vérification sur place, ce registre se trouvant au domicile d'un bénévole de l'association ;

Considérant qu'il y a lieu de prendre acte de ces explications et en particulier de ce que les représentants de la Maison des artistes ont déclaré ne plus utiliser le fichier des assurés pour adresser aux artistes assurés sociaux non membres de l'association des informations à caractère associatif ; Considérant qu'aux termes de l'article 5b de la Convention du Conseil de l'Europe susvisée « les données à caractère personnel faisant l'objet d'un traitement automatisé sont enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités » ;

Considérant qu'il convient de rappeler au président de la Maison des artistes que le fichier de sécurité sociale des artistes plasticiens ne peut être utilisé que pour l'exercice des missions de protection sociale telles que définies par le code de la sécurité sociale ;

Considérant ainsi que ce fichier ne doit pas être utilisé pour adresser aux assurés sociaux des informations à caractère politique, syndical ou associatif, une telle pratique étant de nature à constituer un détournement de finalité passible des sanctions prévues par l'article 226-21 du code pénal ;

Rappelle à la Maison des artistes que les informations enregistrées dans un fichier ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été recueillies.

Chapitre 8

AIDE SOCIALE

I. LA GESTION DU RMI

A. Le fichier national des bénéficiaires du RMI

Le revenu minimum d'insertion a généré, depuis sa création en 1988 et sa pérennisation en 1992, de multiples traitements informatiques, montrant tout à la fois l'importance de l'informatique dans la gestion des données sociales et l'ampleur des dispositifs de surveillance de certaines populations. À cet égard, le fichier national des bénéficiaires du RMI constitue sans aucun doute la clef de voûte d'un système de contrôle a *posteriori* de l'attribution d'une allocation de subsistance dont le versement doit être effectué rapidement. Rappelons que le RMI est versé sous condition de ressources, à un seul allocataire par foyer, majoré par le nombre de personnes à charge. Le fichier national a été conçu pour détecter les éventuelles multi-affiliations au RMI mais, par la suite, les pouvoirs publics ont souhaité compléter ce dispositif d'envergure nationale par une série d'interconnexions impliquant divers organismes concernés par l'attribution du RMI *[cf.* 16e rapport, p. 339). Quoi qu'il en soit, et sans contester la nécessité de lutter contre la fraude, la CNIL a toujours rappelé le droit des plus démunis au respect de leur vie privée (cf. 10e rapport, p. 17 et 15e rapport, p. 106).

En 1997, la CNIL a été saisie de la mise en œuvre à titre définitif du fichier national des bénéficiaires du RMI et, à sa demande, d'un bilan de l'application temporaire du système, qui a révélé, à l'encontre d'une idée qui tendait à se répandre, un nombre faible de multi-affiliations ; néanmoins, le fichier national apparaît bien comme l'outil indispensable pour lutter contre la fraude éventuelle, notamment au regard de la spécificité du RMI du fait d'une ouverture aisée et rapide des droits.

À l'occasion de l'examen de cette demande de pérennisation du fichier national des bénéficiaires du RMI, à laquelle elle a donné un avis favorable, la Commission a relevé d'importantes modifications dans les modalités d'accès et d'utilisation du fichier.

Ainsi, les caisses d'allocation familiale (CAF), principaux organismes payeurs du RMI, pourront désormais interroger, directement et en temps réel, le fichier avant toute affiliation. Les CAF, qui en tout état de cause sont déjà destinataires des informations a *posteriori,* pourront ainsi effectuer leurs recherches, soit sur le NIR, soit sur le nom et la date de naissance, soit sur l'ensemble de ces critères.

La CNAF souhaitait également autoriser certains de ses agents à accéder au fichier national pour pouvoir répondre aux demandes de tiers tels que les autorités judiciaires. La CNIL a estimé qu'une telle demande n'était pas pertinente dans la mesure où les caisses disposant désormais de la faculté d'interrogation du fichier national, toutes pourraient aisément répondre à de telles demandes. La Commission a estimé, enfin, que la CNAF n'avait pas davantage compétence à consulter le fichier national, fût-ce pour vérifier la diligence des caisses à traiter les cas de multi-affiliations signalés : la CNIL a souligné que la CNAF dispose de suffisamment de données statistiques par caisse pour contrôler l'activité des CAF.

Délibération n° 97-052 du 30 juin 1997 portant avis sur la demande présentée par la caisse nationale des allocations familiales (CNAF) relative au fichier national de contrôle des bénéficiaires du revenu minimum d'insertion (RMI)

(Demande d'avis n° 495 432)

La Commission nationale de l'informatique et des libertés,

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 loi n° 88-1088 du 1er décembre 1988 modifiée relative au revenu minimum d'insertion ;

Vu l'arrêté du 4 décembre 1989 relatif à la mise en œuvre d'un contrôle national des attributions multiples de revenu minimum d'insertion ;

Vu le code de la sécurité sociale ;

Vu la délibération n° 89-36 du 25 avril 1989 relative au fichier national de contrôle des bénéficiaires du revenu minimumd'insertion (demande d'avis n° 107 452) ;

Vu le projet d'acte réglementaire relatif à la gestion du fichier national des bénéficiaires du revenu minimum d'insertion, présenté par la caisse nationale des allocations familiales (dite ci-après CNAF) ;

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

Considérant que la CNAF a saisi la Commission d'une demande d'avis relative à la gestion du fichier national de contrôle des bénéficiaires du revenu minimum d'insertion ; que cette demande vise à pérenniser le fichier national qui a été mis en oeuvre/à titre temporaire, par la CNAF après avoir recueilli un avis favorable de la Commission en date du 25 avril 1989 ;

Considérant que le traitement a pour finalité principale de permettre la détection des affiliations multiples au titre du revenu minimum d'insertion, et leur signalement aux caisses d'allocations familiales et caisses de mutualité sociale agricole concernées, ainsi que la production de statistiques ;

Considérant qu'à cette fin, le traitement assurera la centralisation de données relatives aux bénéficiaires du revenu minimum d'insertion, extraites des fichiers des organismes de base ;

Considérant que les informations sont transmises au centre serveur national et concernent exclusivement les données relatives à l'identité de l'allocataire et de son conjoint ou concubin (nom, prénom, date de naissance, numéro d'allocataire, code INSEE de la commune de résidence, code organisme, NIR de l'allocataire et de son conjoint ou concubin), à leur situation familiale (code situation, nombre d'enfants et de personnes à charge) et aux prestations servies (date de la demande, code bénéficiaire/conjoint, date d'ouverture du droit ou de fin de charge, code motif de fin de droit) ;

Considérant que ces informations sont nécessaires au contrôle des multi-affiliations ; qu'en particulier, les informations relatives à l'identité du conjoint ou concubin sont pertinentes dans la mesure où elles permettent de s'assurer qu'au sein d'un même couple, une seule personne reçoit l'allocation ; Considérant que ces informations ne sont pas conservées au-delà du délai de douze mois après la fin du droit ;

Considérant, dans ces conditions, que le principe d'un tel fichier destiné à lutter contre la fraude est légitime ;

Considérant que tous les mois le centre serveur national transmet sur support papier la liste des multi-affiliations aux caisses concernées ;

Considérant qu'indépendamment de la procédure mensuelle de détection des multi-affiliations par le centre serveur national, le fichier pourra être interrogé directement par les agents habilités de chaque caisse d'allocation familiale ; qu'ainsi, les caisses disposeront d'un outil d'interrogation leur permettant de vérifier, lors de chaque demande d'affiliation et avant mise en paiement de l'allocation, que le demandeur, ou son conjoint ou concubin, ne bénéficie pas de droits ouverts auprès de la même caisse ou d'une autre caisse ; que le directeur de chaque caisse tiendra à jour le fichier nominatif des autorisations de consultation délivrées aux agents concernés ; que cet accès direct, dans ces conditions, au fichier national par des agents habilités des caisses est légitime ;

Considérant que la CNAF souhaite autoriser certains de ses agents à accéder aux données nominatives contenues dans le fichier national pour les besoins du suivi des contrôles des multi-affiliations par les caisses concernées, ainsi que pour répondre à des interrogations formulées par des tiers autorisés ;

Considérant que la demande d'accès aux informations nominatives issues du fichier national présentée à ce titre par la caisse nationale n'aurait d'autre objet que de contrôler l'activité des caisses locales et la diligence mise par elles à traiter les cas de multi-affiliations ;

Considérant qu'il y a lieu de souligner que la CNAF dispose déjà de données anonymes lui permettant de connaître le nombre total de multi-affiliations et le nombre de multi-affiliations par caisse ; qu'ainsi la CNAF dispose, d'ores et déjà, des moyens propres à vérifier la diligence des caisses sans qu'il lui soit nécessaire d'accéder aux données nominatives ; Considérant, en outre, que le dispositif désormais envisagé qui permettra à chaque caisse de disposer d'un accès direct au fichier national paraît suffisant pour lutter contre la fraude sans qu'il soit nécessaire que la CNAF dispose d'informations nominatives sur les cas de multi-affiliations ;

Considérant que la CNAF fait valoir en outre qu'un accès au fichier nominatif permettrait de mieux répondre aux interrogations formulées par les tiers autorisés, et tout particulièrement dans le cadre d'une enquête judiciaire : que cependant les caisses locales disposant désormais d'un accès direct et en temps réel au fichier national, cette demande de la caisse nationale n'est pas justifiée ; qu'il suffira en effet aux tiers autorisés de s'adresser auprès de n'importe quelle caisse afin d'avoir accès aux informations sollicitées ;

Considérant, enfin, qu'aux termes de l'article 21 de la loi du 1er décembre 1988 modifiée, les organismes payeurs chargés du versement de l'allocation ne peuvent communiquer les informations recueillies dans l'exercice de leur mission qu'au représentant de l'État dans le département, au président du conseil général et au président de la commission locale d'insertion ainsi que la liste des bénéficiaires *aux* présidents des centres communaux d'action sociale et aux organismes instructeurs concernés ;

Considérant que toute personne justifiant de son identité peut exercer son droit d'accès aux informations nominatives la concernant contenues dans le fichier central et, le cas échéant, en obtenir communication auprès de l'organisme de base auprès duquel il est rattaché ;

Émet un avis favorable au projet d'acte réglementaire présenté par la caisse nationale des allocations familiales concernant le fichier national de contrôle des bénéficiaires du revenu minimum d'insertion, sous réserve des modifications suivantes :

- à l'article 1er, dernier alinéa, les mots «et par la CNAF» soient supprimés,
- à l'article 4, dernier alinéa, les mots « de la CNAF » soient supprimés,
- à l'article 5, premier alinéa, le tiret « soit auprès de la CNAF — 23, rue Daviel 75634 Paris cedex 13 » soit supprimé.

B. Les commissions locales d'insertion

Dans la mesure où ils doivent conduire ensemble et contractuellement l'action d'insertion sociale et professionnelle des bénéficiaires du RMI, l'État et le département sont co-décisionnaires de la politique d'insertion à mener au niveau local. Pour leur part, les commissions locales d'insertion (CLI) ont la mission de proposer une mesure d'insertion concrétisée par un contrat établi

avec l'allocataire dans un délai de trois mois, afin de permettre au représentant de l'État de proroger le droit à l'allocation, d'évaluer les besoins d'insertion sociale et professionnelle des bénéficiaires du RMI, en vue d'élaborer un programme local d'insertion destiné à assurer l'offre d'insertion adaptée aux bénéficiaires du RMI.

Le conseil général et la préfecture des Alpes-Maritimes ont saisi la CNIL d'un projet d'informatisation des procédures liées au revenu minimum d'insertion dans ce département. Il s'agit principalement de la mise en place d'un fichier centralisé au niveau départemental, commun aux huit commissions locales d'insertion du département, dont la moitié est gérée par l'État ; l'outil informatique doit aussi assurer le suivi des actions d'insertion proposées dans le cadre des contrats passés avec les bénéficiaires de l'allocation de RMI. Enfin, l'application ainsi partagée selon une procédure d'identification et d'habilitation des intervenants au dispositif, vise à la production de statistiques locales destinées à offrir un meilleur programme départemental d'insertion.

Bien que l'idée d'individualiser le coût des actions d'insertion engagées par le département ait été totalement abandonnée, la CNIL a néanmoins estimé que l'anonymisation des informations utilisées pour l'élaboration des statistiques devait se conformer à des règles très strictes. La Commission a ainsi rappelé la nécessité qu'après croisement des données, aucun dénombrement inférieur à cinq individus ne soit communiqué ; de même, au niveau infra-communal, le nombre d'individus concernés doit être supérieur à cent. Également dans le souci de préserver la confidentialité d'informations par nature sensibles, la CNIL a demandé que la durée de conservation des données dans le traitement, initialement égale à la durée de vie du dossier, soit réduite et affinée selon les normes habituellement préconisées par la CNIL en matière de RMI.

En définitive, et tout en mettant l'accent sur l'importance des mesures de sécurité dans une application conçue pour que de nombreuses personnes y accèdent en fonction de leurs habilitations respectives, la CNIL a donné un avis favorable au projet conjoint du président du conseil général et du préfet des Alpes-Maritimes.

Délibération n° 97-022 du 1er avril 1997 portant avis sur la demande présentée conjointement par le conseil général des Alpes-maritimes et la préfecture des Alpes-maritimes et concernant la mise en œuvre d'un traitement automatisé de données nominatives relatif à la gestion des commissions locales d'insertion et le suivi de l'insertion
(Demande d'avis n° 457 715)

La Commission nationale de l'informatique et des libertés,

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 loi n° 88-1088 du 1er décembre 1988 modifiée, relative au revenu minimum d'insertion ;

Vu le décret n° 94-632 du 19 juillet 1994 relatif à la nature des informations transmises par les collectivités publiques et les organismes associés aux fins d'établissement de statistiques sur le revenu minimum d'insertion ;

Vu l'arrêté du 20 septembre 1994 relatif au traitement informatisé à des fins statistiques des informations contenues dans les bulletins de situation des bénéficiaires du revenu minimum d'insertion ;

Vu les projets d'actes réglementaires présentés par le président du conseil général des Alpes-Maritimes et le préfet des Alpes-Maritimes ;

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 des Alpes-Maritimes et la préfecture des Alpes-Maritimes ont saisi la Commission d'une demande d'avis concernant un traitement automatisé d'informations nominatives destiné à gérer l'activité des commissions locales d'insertion dans le département et permettre un suivi des actions d'insertion, tant par les commissions locales d'insertion, que par les services du conseil général chargés de l'insertion et du paiement des actions individuelles ;

Considérant que ce traitement a également pour finalités l'élaboration de statistiques locales destinées notamment au programme départemental d'insertion, conformément aux dispositions du décret du 19 juillet 1994, susvisé, à savoir la production de tableaux relatifs à l'activité des commissions locales d'insertion et des informations individuelles afin d'élaborer des statistiques pour le programme départemental d'insertion et les programmes locaux d'insertion tels qu'ils sont respectivement définis aux articles 36 et 42-1 de la loi du 1er décembre 1988 modifiée ;

Considérant que les statistiques produites pourront porter sur des variables socio-démographiques relatives à l'âge, au niveau de formation, à la composition familiale, aux domaines d'action d'insertion, au secteur d'intervention de la commission locale d'insertion, la commune et l'îlot INSEE pour les communes importantes du département ; qu'il convient, à cet égard, que toutes mesures soient prises afin de garantir l'anonymat de ces statistiques ;

Considérant, en outre, que le conseil général et la préfecture se sont engagés à ne traiter, ni produire aucune information susceptible de permettre l'individualisation, pour chaque bénéficiaire, du coût de l'action sociale engagée par le département, au titre de l'insertion et de l'aide médicale ;

Considérant que les catégories d'informations sont relatives à l'identité de la personne, son adresse, sa situation familiale, sa situation financière, son inscription à l'agence locale pour l'emploi, sa qualification, ses besoins d'insertion, les avis de la commission locale d'insertion, les actions et facilités prévues par le contrat d'insertion, l'existence d'un problème de santé ; que ces catégories d'informations collectées sont pertinentes et non excessives au regard de la finalité poursuivie ;

Considérant que les destinataires des informations sont, dans la limite de leurs attributions, les agents des secrétariats et les membres des commissions locales d'insertion, les agents habilités de la délégation à l'insertion et à la lutte contre l'exclusion du département ainsi que le chargé de mission auprès du représentant de l'État dans le département ; que peuvent être destinataires des informations traitées, les agents habilités du service départemental de l'aide sociale générale pour le bénéfice de l'aide médicale et, le cas échéant, la prise en charge des cotisations d'assurance personnelle, la caisse d'allocations familiales pour les renouvellements de l'allocation, l'agence locale pour l'emploi dans la mesure où elle participe à la réalisation du contrat d'insertion, le service de l'urbanisme et du logement de la préfecture en ce qui concerne les informations relatives à l'identité et la situation des bénéficiaires lorsque ceux-ci connaissent des problèmes de logement, la cellule d'appui santé et le centre de santé en ce qui concerne les informations relatives à l'identité des bénéficiaires lorsque ceux-ci présentent des problèmes de santé, ainsi que la direction départementale du travail, de l'emploi et de la formation professionnelle pour les informations relatives aux bénéficiaires de contrats aidés ;

Considérant que le droit d'accès et de rectification des personnes intéressées, prévu en application des articles 34, 35 et 36 de la loi du 6 janvier 1978, s'exerce auprès du président de la commission locale d'insertion compétente, auprès du président du conseil général ou auprès du chargé de mission RMI auprès du préfet ;

Considérant que les intéressés doivent être informés clairement de la liste des destinataires des informations collectées ainsi que de la nature des données qui leur sont communiquées ;

Considérant que la responsabilité de la collecte et de la transmission des données nominatives échoit aux présidents des commissions locales d'insertion compétents ;

Considérant que les informations nominatives sont conservées jusqu'à l'expiration d'un délai d'un an après la clôture du dossier du bénéficiaire ; que les informations relatives aux demandeurs ayant fait l'objet d'une décision de refus d'ouverture de droit sont effacées six mois après la décision du préfet ; qu'en début de chaque année, les données financières relatives aux prestations facturées pour chaque bénéficiaire, dans le cadre des mesures d'insertion proposées, seront anonymisées, tout en conservant, de façon nominative, les données correspondant à l'exercice comptable précédent ;

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 de d'autorisations personnalisées ;

Considérant que, s'agissant d'une application fonctionnant selon une architecture client/serveur, toutes garanties doivent être prises afin notamment d'éviter le rapatriement, sans contrôle, des données de la base afin de reconstituer des fichiers nominatifs ;

Considérant que dans la mesure où la responsabilité de la mise en œuvre du traitement incombe au président du conseil général et au représentant de l'État dans le département, le projet d'acte réglementaire doit prendre la forme d'un projet d'arrêté conjoint du président du conseil général des Alpe-Maritimes et du préfet des Alpes-Maritimes ;

Rappelle que les règles suivantes doivent être respectées afin d'assurer l'anonymisation des statistiques :
— après croisement des données, aucun dénombrement inférieur à cinq individus n'est communiqué ;
— au niveau infra-communal, le nombre d'individus concernés doit être supérieur à cent et aucun dénombrement inférieur à cinq individus, après croisement des données, ne peut être communiqué.
Émet un avis favorable à la demande présentée conjointement par le président du conseil général des Alpes-Maritimes et le préfet du département des Alpes-Maritimes et concernant la mise en œuvre d'un traitement automatisé de données nominatives relatif à la gestion des commissions locales d'insertion et du suivi des actions d'insertion.

II. LE DEVELOPPEMENT DES BASES DE DONNÉES SOCIALES DANS LES DÉPARTEMENTS

A. La gestion centralisée des données

Dans le domaine de l'action sociale, l'informatique tend à jouer un rôle prépondérant, notamment comme outil d'évaluation et d'aide à la décision. Les départements, qui sont compétents depuis la décentralisation en matière d'action sociale, souhaitent recourir à des outils informatiques de suivi de leur politique sociale, notamment pour contenir les dépenses connexes. Aussi, depuis quelques années, plusieurs départements ont mis en place, après avis de la CNIL, un fichier unique des bénéficiaires des différentes prestations assurées par le département au titre de l'action sociale. Pour l'essentiel, cela a été réalisé grâce à une application dénommée « ANIS », qui revêt la particularité d'être constituée selon une architecture client/serveur (cf. 15e rapport, p. 122, 16e rapport, p. 323, 17e rapport, p. 296).

En 1997, la CNIL a été saisie du système «ANIS» dans d'autres départements, parfois dans des fonctionnalités inexploitées jusqu'à présent. Ainsi, la CNIL s'est prononcée favorablement sur l'utilisation d'« ANIS » dans le domaine de l'aide sociale à l'enfance, dans les départements du Rhône et de l'Ain. Il s'agit non seulement de gérer les procédures liées aux missions de l'aide à l'enfance, mais également une partie des procédures d'action sociale de terrain, en amont des décisions administratives (placement, suivi...). De même, la CNIL a donné avis favorable à la demande d'informatisation de l'aide générale départementale dans le Tarn. Enfin, l'expérimentation de l'application dans l'Ain, qui a débuté en 1995, a été prolongée d'une année supplémentaire, l'ampleur du projet posant en pratique de sérieuses difficultés.
Dans tous les cas, la CNIL ne s'est pas montrée hostile au principe d'une mise en commun par les services du département, d'informations en nombre

limité concernant les bénéficiaires d'actions sociales. Toutefois, la Commission demeure extrêmement vigilante quant au partage d'informations entre les différents services concernés du département afin qu'il ne porte pas atteinte à la confidentialité des données collectées. De même, la Commission reste attentive aux destinataires des informations et à leurs habilitations respectives, mais également à la durée de conservation des données. La CNIL manifeste aussi une vigilance particulière quant à l'utilisation des zones bloc-notes de l'application.

La Commission souhaite enfin contrôler de très près le développement des applications de cette nature afin que l'informatisation accrue des services sociaux, aussi justifiée qu'elle soit, ne devienne pas un carcan administratif ou bureaucratique susceptible de dénaturer les difficiles missions qu'accomplissent les services sociaux au service de la solidarité nationale.

Délibération n° 97-006 du 4 février 1997 portant avis sur la demande présentée par le conseil général du Rhône et concernant la gestion informatisée de l'aide sociale à l'enfance et de l'action sociale de terrain « ANIS-ASE »

(Demande d'avis n° 496 142)

La Commission nationale de l'informatique et des libertés,

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 loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu les lois de décentralisation n° 83-8 du 7 janvier 1983 et n° 83-663 du 22 juillet 1983 ;

Vu la loi n° 86-17 du 6 janvier 1986 relative au transfert de compétence en matière sanitaire et sociale ;

Vu le décret n° 96-793 du 12 septembre 1996 relatif à l'autorisation d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques ;

Vu le titre II du code de la famille et de l'aide sociale relatif à l'action sociale en faveur de l'enfance et de la famille ;

Vu le projet d'acte réglementaire présenté le 28 janvier 1997 par le conseil général au Rhône ;

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 du Rhône a saisi la Commission d'une demande d'avis relative à l'informatisation de la gestion de l'aide sociale à l'enfance ; que ce traitement automatisé de données nominatives intitulé « ANIS-ASE » assure, à titre principal, la gestion des missions du conseil général en matière d'aide sociale à l'enfance et à la famille, à savoir la mise en œuvre et la gestion des procédures d'attribution des prestations

d'aide sociale à l'enfance et à la famille, la gestion des informations relatives aux usagers bénéficiant des prestations d'aide sociale à l'enfance et à la famille et des actions sociales de terrain ainsi que la gestion financière et comptable du service ;

Considérant que le traitement consiste en une base de données unique, mise à disposition des agents départementaux affectés aux missions de protection de l'enfance et à l'action sociale de terrain, dans la limite de leurs attributions et consultable selon une procédure d'habilitation particulière ; que seuls les personnels directement concernés par le dossier sont habilités à consulter, modifier ou créer dans l'application des informations nominatives relatives aux enfants en difficulté, aux difficultés rencontrées par les personnes suivies, à la définition des objectifs et projets et à leur évaluation ; que la saisine de ces dernières informations revêt un caractère facultatif et que les informations telles qu'elles résultent des différentes rubriques 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 en outre que les travailleurs sociaux disposent d'une zone de texte libre destinée à dresser un diagnostic sur la situation rencontrée ; que toutes dispositions doivent être prises afin que ne soient portées dans le traitement que des informations aisément vérifiables et accessibles aux intéressés ; considérant, en outre, que ces informations seront systématiquement supprimées de l'application dès lors que la mesure visée ou l'objectif sera atteint ;

Considérant que les informations enregistrées sont relatives à l'identification des personnes bénéficiaires de prestations du service de l'aide sociale à l'enfance ou d'actions sociales de terrain, de leur situation économique et financière, de leur vie professionnelle et des enfants pris en charge par le service de l'aide sociale à l'enfance ; qu'en outre peuvent être enregistrées, à l'initiative du travailleur social en charge du dossier et selon une nomenclature de codes arrêtée par le responsable du traitement et communiquée à la Commission, des indicateurs relatifs à la nature des difficultés rencontrées, à l'objectif à atteindre et à l'évaluation du travail social ; que les informations en rapport avec la justice concernent toutes les décisions prises par l'autorité judiciaire concourant aux missions de protection de l'enfance ; que le numéro de sécurité sociale est utilisé dans le cadre des missions d'aide sociale à l'enfance, lorsqu'il y a récupération auprès des caisses de sécurité sociale des prestations servies par les services ou lorsque les cotisations de sécurité sociale des bénéficiaires de l'aide sociale à l'enfance sont payées par les services ;

Considérant que les destinataires des informations sont, dans la limite de leurs attributions, les agents du département participant aux missions de protection de l'enfance et à l'action sociale de terrain, à l'exclusion des informations relatives à la nature des difficultés rencontrées, à l'objectif à atteindre et à l'évaluation du travail social qui sont réservées aux seuls travailleurs sociaux en charge du dossier ; que peuvent être destinataires des informations traitées, les représentants de l'autorité judiciaire concourant aux missions de protection de l'enfance, les personnels habilités des organismes sociaux compétents, à savoir, notamment, la caisse primaire d'assurance maladie, la caisse d'allocations familiales, le Centre communal d'action sociale, l'association collective d'aide au logement et les associations caritatives, dans la limite de leurs attributions et pour les informations les concernant, ainsi que les personnels habilités du service des finances et

du budget du département pour les informations nécessaires aux procédures de mandatement et de suivi financier et de la paierie départementale du Rhône pour les informations nécessaires à la mise en paiement des prestations financières ;

Considérant que les données relatives aux procédures d'aide sociale à l'enfance sont conservées pendant vingt-quatre mois après la date de fin d'effet de la dernière prestation accordée à l'individu ; que les données relatives aux procédures d'action sociale de terrain sont conservées dix-huit mois après la date de fin d'effet de la procédure ; que les données nominatives concernant le ou les individus du dossier familial seront supprimées dès lors qu'aucune procédure n'est en cours et au terme des délais précédents ;

Considérant que le droit d'accès et de rectification des personnes intéressées, prévu en application des articles 34, 35 et 36 de la loi du 6 janvier 1978, s'exerce auprès du responsable de la maison du département du Rhône dont dépend l'usager ou auprès des services départementaux chargés de la vie sociale ;

Considérant que toutes dispositions doivent être prises afin d'informer clairement les usagers des destinataires des informations et des droits qui leur sont offerts au titre de la loi du 6 janvier 1978 et notamment de leur droit de s'opposer, pour des raisons légitimes, à l'informatisation et à la consultation de leurs données personnelles par des services étrangers à l'instruction ou à la gestion de leur demande ;

Considérant que des mesures de sécurité ont été prévues, notamment pour assurer un accès différencié des informations selon les habilitations des agents, sous forme de codes d'identification et d'autorisations personnalisés ; considérant que l'application a été conçue de façon à interdire aux utilisateurs d'extraire des données de la base afin de reconstituer des fichiers nominatifs, sans contrôle ;

Émet un avis favorable au projet d'arrêté présenté par le président du conseil général du Rhône concernant la mise en oeuvre d'un traitement automatisé de données nominatives relatif à la gestion de l'aide sociale à l'enfance et de l'action sociale de terrain.

Délibération n° 97-030 du 6 mai 1997 portant avis sur la demande présentée par le conseil général du Tarn et concernant l'informatisation de l'aide sociale générale départementale « PHILEAS-ASG »

(Demande d'avis n° 491 791)

La Commission nationale de l'informatique et des libertés,

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 loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi n° 83-663 du 22 juillet 1983 complétant la loi n° 83-08 du 7 janvier 1983 relative à la répartition des compétences entre les communes, les départements, les régions et l'État ;

Vu la loi n° 86-17 du 6 janvier 1986 relative au transfert de compétences en matière sanitaire et sociale ;

Vu le décret n° 96-793 du 12 septembre 1996 relatif à l'autorisation d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques ;

Vu le projet d'acte réglementaire présenté par le président du conseil général du Tarn ;

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 du Tarn a saisi la Commission d'une demande d'avis relative à la gestion de l'aide sociale générale départementale ; que ce traitement automatisé de données nominatives intitulé PhiléAS-ASG assure, à titre principal, la gestion des prestations du titre III du code de la famille et de l'aide sociale qui sont mises à la charge des départements en vertu des lois susvisées sur la décentralisation, à savoir, les demandes d'aide médicale, d'aide sociale aux personnes âgées et d'aide sociale aux personnes handicapées ainsi que la gestion financière et comptable du service ;

Considérant que les informations nominatives sont relatives à l'identification des personnes sollicitant une prestation d'aide sociale, de leur situation familiale, économique et financière, de leur vie professionnelle, de leur couverture sociale, ainsi que des informations concernant l'identification du représentant légal ou tuteur du demandeur et des informations concernant l'identité des obligés alimentaires, leur adresse, le lien de parenté avec le bénéficiaire et le montant de la participation : que sont enregistrées également les informations relatives à l'identité de l'agent instructeur de la demande ainsi que l'identité, l'adresse, les références bancaires, la catégorie professionnelle des fournisseurs ou prestataires ;

Considérant que le service d'aide sociale générale est habilité par le décret du 12 septembre 1996 à consulter et enregistrer le numéro de sécurité sociale, dans le cadre de ses relations directes avec les organismes de protection sociale ;

Considérant que les destinataires des informations sont, dans la limite de leurs attributions, les agents du département affectés au service de l'aide sociale générale, ainsi que les agents des services financiers chargés du mandatement et du paiement des prestations financières de l'aide sociale générale et les personnels habilités des centres communaux d'action sociale ; que peuvent être destinataires des informations traitées, dans la stricte limite des nécessités du traitement d'une demande d'aide sociale, les membres des commissions d'admission et des commissions techniques, les personnels habilités des organismes de protection sociale et de recouvrement des cotisations d'assurance personnelle, des établissements d'hébergement en cas de placement au titre de l'aide sociale, des établissements d'hospitalisation, et enfin, de la direction départementale des affaires sanitaires et sociales du Tarn et les services sociaux des autres départements en cas de transfert ;

Considérant que l'article 3 du projet d'arrêté doit être complété de façon à préciser que, seuls, les agents Viabilités des organismes et services précités peuvent être destinataires des informations ;

Considérant que le traitement dispose d'une zone de texte libre ; que toutes dispositions doivent être prises afin que n'y soient portées que des informations à caractère administratif destinées à apprécier le droit aux prestations et accessibles aux intéressés à l'exclusion de toute appréciation subjective et de toute information relevant de l'article 31 de la loi du 6 janvier 1978 ;

Considérant que les données nominatives sont conservées pendant vingt-quatre mois après la date de fin d'effet de la dernière prestation accordée à l'individu ou au dernier individu concerné du dossier familial ; qu'en ce qui concerne les dossiers qui donnent lieu à recours sur succession, les informations nominatives peuvent être conservées jusqu'à la fin de l'opération de recette liée au recours sur succession ;

Considérant que le droit d'accès et de rectification des personnes intéressées, prévu en application des articles 34, 35 et 36 de la loi du 6 janvier 1978 s'exerce directement auprès du directeur de la solidarité du département du Tarn, chargé de l'aide sociale générale, ou par l'intermédiaire du Centre communal d'action sociale dont ils relèvent ;

Considérant que des mesures de sécurité ont été prévues pour assurer la confidentialité des données ; que l'application a été conçue de façon à interdire aux utilisateurs d'extraire des données de la base afin de reconstituer des fichiers nominatifs, sans contrôle ; qu'en outre il est procédé à des fins de sécurité, à une journalisation des interrogations permettant l'enregistrement, pendant un mois, des noms, numéros de postes clients, des dates et heures, et codes des transactions utilisées ;

Émet un avis favorable au projet d'arrêté présenté par le président du conseil général du Tarn concernant la mise en oeuvre d'un traitement automatisé de données nominatives relatif à la gestion de l'aide sociale départementale, sous réserve :
- que l'article 3 du projet d'arrêté soit complété de façon à préciser que seuls les agents habilités des services et organismes énumérés dans cette disposition peuvent être destinataires des informations ;
- que l'attention des utilisateurs du traitement soit appelée sur la nécessité de n'enregistrer dans la zone bloc-notes que les informations à caractère administratif destinées à apprécier le droit aux prestations et accessibles aux intéressés, à l'exclusion de toute appréciation subjective et de toute information relevant de l'article 31 de la loi du 6 janvier 1978.

Délibération n° 97-061 du 8 juillet 1997 portant avis sur la demande présentée par le conseil général de l'Ain concernant la prorogation de l'expérimentation du traitement automatisé relatif à la gestion de l'action sociale départementale, dénommé « Approche nouvelle de l'information sociale « ANIS » »

La Commission nationale de l'informatique et des libertés,

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 les lois de décentralisation n° 83-8 du 7 janvier 1983 et n° 83-663 du 22 juillet 1983 ;

Vu les délibérations n° 95-065 du 23 mai 1995 et 96-058 du 9 juillet 1996 (demande d'avis n° 363 906) ;

Vu le projet d'acte réglementaire présenté par le président du 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 par délibérations du 23 mai 1995 et 9 juillet 1996, la Commission a autorisé la mise en œuvre, pour une durée limitée prenant fin au plus tard le 30 juin 1997, d'un traitement automatisé de données nominatives relatif à la gestion de l'action sociale départementale, dénommé « ANIS », devant permettre aux responsables du projet d'apprécier l'adéquation du traitement aux besoins des services utilisateurs ;

Considérant que la mise en oeuvre de cette expérimentation, qui a connu de nombreux retards, n'a pas permis au conseil général de l'Ain d'évaluer toutes les fonctionnalités initialement envisagées ;

Considérant que la Commission est saisie par le département de l'Ain d'une demande de prorogation destinée à poursuivre l'expérimentation ;

Émet un avis favorable pour une durée limitée, prenant fin le **31 mars 1998** au traitement automatisé de données nominatives mis en œuvre dans les circonscriptions de Belley, Bourg-en-Bresse et Chatillon-sur-Chalaronne, relatif à la gestion de l'action sociale départementale, dénommé « ANIS ».

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 à l'enfance et de l'action sociale de terrain « ANIS-ASE »

(Demande d'avis n° 532 096)

La Commission nationale de l'informatique et des libertés,

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 loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu les lois de décentralisation n° 83-8 du 7 janvier 1983 et n° 83-663 du 22 juillet 1983 ;

Vu la loi n° 86-17 du 6 janvier 1986 relative au transfert de compétence en matière sanitaire et sociale ;

Vu le décret n° 96-793 du 12 septembre 1996 relatif à l'autorisation d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques ;

Vu le titre II du code de la famille et de l'aide sociale relatif à l'action sociale en faveur de l'enfance et de la famille ;

Vu les délibérations n° 095-065 du 23 mai 1995, 96-058 du 9 juillet 1996 et 97-061 du 8 juillet 1997;

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 de l'aide sociale à l'enfance ; que ce traitement automatisé de données nominatives intitulé ANIS-ASE assure, à titre principal, la gestion des missions du conseil général en matière d'aide sociale à l'enfance et à la famille, à savoir la mise en oeuvre et la gestion des procédures d'attribution des prestations d'aide sociale à l'enfance et à la famille, la gestion des informations relatives aux usagers bénéficiant des prestations d'aide sociale à l'enfance et à la famille et des actions sociales de terrain ainsi que la gestion financière et comptable du service ;

Considérant que le traitement consiste en une base de données unique, mise à la disposition, dans la limite de leurs attributions, des agents départementaux affectés aux missions de protection de l'enfance et à l'action sociale de terrain et consultable selon une procédure d'habilitation particulière ; que seuls les personnels directement concernés par le dossier sont habilités à consulter, modifier ou créer dans l'application les informations nominatives relatives à la nature des difficultés rencontrées par les personnes suivies, de leurs potentialités, ainsi qu'à la définition des objectifs à atteindre et à leur évaluation ; que la saisie de ces dernières informations revêt un caractère facultatif et que les informations telles qu'elles résultent des différentes rubriques 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 les informations recueillies au titre de l'action sociale pourraient faire l'objet d'une exploitation statistique et anonyme, susceptible d'être utilisée par les services du conseil général afin d'évaluer les réponses apportées par les services sociaux aux problèmes rencontrés par les usagers ;

Considérant que, compte tenu du caractère facultatif de la saisie de certaines informations et du caractère subjectif de certaines codifications, l'exploitation, par le conseil général, de ces statistiques ne peut constituer un instrument de mesure de l'activité des travailleurs sociaux et des caractéristiques de la population suivie ;

Considérant en outre que les travailleurs sociaux disposent de zones de texte libre destinées à dresser un diagnostic sur la situation rencontrée, ainsi qu'à compléter l'évaluation du travail social ; que toutes dispositions doivent être prises afin que ne soient portées dans ces zones de texte libre que des informations aisément vérifiables et accessibles aux intéressés ; qu'il résulte de la demande d'avis que ces informations seront systématiquement suppri-

mées de l'application dès lors que la mesure visée sera accomplie ou l'objectif atteint ;

Considérant que les informations enregistrées sont relatives à l'identification des personnes bénéficiaires de prestations du service de l'aide sociale à l'enfance ou d'actions sociales de terrain, de leur situation économique et financière, de leur vie professionnelle et des enfants pris en charge par le service de l'aide sociale à l'enfance ; qu'en outre peuvent être enregistrées, à l'initiative du travailleur social en charge du dossier et selon une nomenclature de codes communiquée à la Commission, des indicateurs relatifs à la nature des difficultés et des potentialités rencontrées, aux objectifs à atteindre et à l'évaluation du travail social ; que les informations en rapport avec la justice concernent toutes les décisions prises par l'autorité judiciaire concourant aux missions de protection de l'enfance ; que le numéro de sécurité sociale est utilisé dans le cadre des missions d'aide sociale à l'enfance, lorsqu'il y a récupération auprès des caisses de sécurité sociale des prestations servies par les services ou lorsque les cotisations de sécurité sociale des bénéficiaires de l'aide sociale à l'enfance sont payées par les services ;

Considérant que les destinataires des informations sont, dans la limite de leurs attributions, les agents du département participant aux missions de protection de l'enfance et à l'action sociale de terrain, à l'exclusion des informations relatives à la nature des difficultés et des potentialités rencontrées, aux objectifs à atteindre et à l'évaluation du travail social qui sont, aux termes du projet d'acte réglementaire soumis à la Commission, réservées aux seuls travailleurs sociaux en charge du dossier ; que peuvent être destinataires des informations traitées, les représentants de l'autorité judiciaire concourant aux missions de protection de l'enfance, les personnels habilités des organismes sociaux compétents, à savoir, la caisse primaire d'assurance maladie, la caisse d'allocations familiale, le centre communal d'action sociale, les associations caritatives, dans la limite de leurs attributions et pour les informations les concernant, ainsi que les personnels habilités du service des finances et du budget du département pour les informations nécessaires aux procédures de mandatement et de suivi financier et de la paierie départementale de l'Ain pour les informations nécessaires à la mise en paiement des prestations financières ;

Considérant que les données relatives aux procédures d'aide sociale à l'enfance sont conservées pendant vingt-quatre mois après la date de fin d'effet de la dernière prestation accordée à la personne concernée ; que les données relatives aux procédures d'action sociale de terrain sont conservées dix-huit mois après la date de fin d'effet de la procédure ; que les données nominatives concernant la ou les personnes concernées seront supprimées dès lors qu'aucune procédure n'est en cours et au terme des délais précédents ;

Considérant que le droit d'accès et de rectification des personnes intéressées, prévu en application des articles 34, 35 et 36 de la loi du 6 janvier 1978, 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 offerts au titre de la loi du 6 janvier 1978 et notamment de leur droit d'opposition ;

Considérant que des mesures de sécurité ont été prévues, notamment pour assurer un accès différencié des informations selon les habilitations des agents, sous forme de codes d'identification et d'autorisations personnalisés ; considérant que l'application a été conçue de façon à interdire aux utilisateurs d'extraire des données de la base afin de reconstituer des fichiers nominatifs, sans contrôle ;

Émet un avis favorable au projet d'arrêté présenté par le président du conseil général de l'Ain concernant la mise en oeuvre d'un traitement automatisé de données nominatives relatif à la gestion de l'aide sociale à l'enfance et de l'action sociale de terrain.

B. Le suivi de la prestation spécifique dépendance par carte à puce

Dans le cadre de l'attribution de la prestation spécifique dépendance (PSD) instituée par la loi n° 97-60 du 24 janvier 1997 en faveur des personnes âgées dépendantes et financée par les conseils généraux, le conseil général des Bouches-du-Rhône a souhaité doter les intervenants à ce dispositif, d'outils performants destinés à faciliter la gestion et le suivi des aides à domicile et à en contrôler notamment l'effectivité.

Dans ce cadre, le conseil général a conclu une convention avec une société de services (ADICARTE), chargée, pour le compte du conseil général, de diffuser les cartes à puce fournies aux personnes âgées et d'éditer des relevés mensuels et des statistiques de suivi. De même, chaque organisme prestataire agréé par le conseil général doit passer une convention qui fixe les modalités selon lesquelles la société ADICARTE lui fournit des cartes à puce destinées aux intervenants à domicile et édite des relevés mensuels et des statistiques.

Concrètement, le dispositif « ADICARTE » permet de centraliser dans une base les données transmises par les différents partenaires ; à cet effet, les personnes âgées bénéficiaires de la PSD et les intervenants à domicile (aide ménagère, garde de jour ou de nuit, auxiliaire médical...} utilisent des cartes à puce et des lecteurs qui assurent une mise à jour automatique du suivi de la consommation de l'aide par le bénéficiaire et les intervenants à domicile. Les informations sont ensuite télédéchargées directement chez ADICARTE qui établit le relevé des prestations à destination du financeur (contrôle des heures effectuées par prestataire, suivi de la consommation des prestations par le bénéficiaire de l'allocation), ainsi que le relevé à l'attention du prestataire (contrôle de l'activité des intervenants pour établissement des salaires, suivi de la consommation pour chaque bénéficiaire, préparation de la facturation pour le conseil général). En retour, la société ADICARTE perçoit une rémunération forfaitaire pour chaque heure gérée par le système, répartie entre le prestataire et le financeur.

Au plan de la protection des données personnelles, il apparaît que la société ADICARTE est appelée à ne collecter que des informations très succinctes, transmises soit par le conseil général concernant l'identification des bénéficiaires de la prestation, soit par le prestataire concernant l'identification des différents salariés intervenant auprès des bénéficiaires. Quant aux cartes à puce, elles mentionnent seulement l'identité du bénéficiaire et de l'intervenant et ne conservent en mémoire que des informations sur les droits des bénéficiaires (nombre d'heures par exemple) et les différentes tâches susceptibles d'être accomplies par l'intervenant. À cet égard, la Commission a relevé qu'aucune information à caractère médical concernant le degré de dépendance n'est enregistrée dans la base ; de même, il n'est pas prévu que le numéro de sécurité sociale soit utilisé.

Enfin, agissant comme sous-traitant pour le compte du département et des prestataires de services, la société ADICARTE restitue la totalité des informations qui lui sont confiées et n'effectue aucune transaction pour son propre compte. Dès lors, la Commission ayant estimé que la société ADICARTE ne pouvait être considérée comme responsable du traitement aux termes de la loi du 6 janvier 1978, à savoir la personne disposant du pouvoir de décider la création d'un traitement, la société ADICARTE n'a été soumise à aucune formalité de déclaration.

Après avoir constaté que le dispositif ADICARTE ne pouvait conduire à un « traçage » des intervenants sociaux, la Commission a donné un avis favorable à la mise en œuvre de ce projet, dont elle souhaite recevoir un bilan d'évaluation, sachant que d'autres départements sont intéressés par l'utilisation de ce système.

Délibération n° 97-082 du 21 octobre 1997 portant avis sur la demande présentée par le conseil général des Bouches-du-Rhône et concernant la mise en œuvre d'un traitement automatisé de données nominatives au moyen d'un dispositif de cartes à microprocesseur destiné à assurer la gestion du suivi de la prestation spécifique dépendance
(Demande d'avis n° 528 272)

La Commission nationale de l'informatique et des libertés,

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 loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu la loi n° 83-663 du 22 juillet 1983 complétant la loi n° 83-08 du 7 janvier 1983 relative à la répartition des compétences entre les communes, les départements, les régions et l'État ;

Vu la loi n° 97-60 du 24 janvier 1997 instituant une prestation spécifique dépendance ;

Vu le projet d'acte réglementaire présenté par le président du conseil général des Bouches-du-Rhône ;

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 des Bouches-du-Rhône a saisi la Commission d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé de données nominatives au moyen d'un dispositif de cartes à microprocesseur destiné à assurer la gestion du suivi des aides à domicile accordées aux personnes âgées au titre de la prestation spécifique dépendance instituée par la loi n° 97-60 du 24 janvier 1997 ;

Considérant, en effet, qu'aux termes de la loi n° 97-60 du 24 janvier 1997 instituant la prestation spécifique dépendance, le président du conseil général doit s'assurer, notamment, de l'effectivité de l'aide apportée ; Considérant que ce projet sera réalisé en partenariat avec les organismes prestataires agréés par le conseil général pour assurer auprès des personnes âgées les prestations à domicile ;

Considérant que le dispositif soumis à l'avis de la Commission par le conseil général consiste à doter les personnes âgées concernées de cartes à mémoire comportant leur identification ainsi que la nature de l'aide accordée, et ce à l'exclusion du numéro de sécurité sociale et de toute information de caractère médical ;

Considérant, par ailleurs, qu'il appartiendra à chaque organisme prestataire de doter ses intervenants de lecteurs de cartes portables et de cartes à microprocesseur comportant l'identification et le métier de l'intervenant et de son prestataire ;

Considérant que lors de chaque intervention à domicile, les deux cartes seront successivement introduites dans le lecteur, la carte de l'intervenant n'étant retirée qu'une fois sa tâche accomplie : qu'ainsi, le lecteur mémorisera pour chaque bénéficiaire les date et heures de l'intervention ainsi que le temps effectué ;

Considérant que ces informations seront télé-transmises à un prestataire de services chargé d'effectuer pour le compte du conseil général et de chaque organisme prestataire la comptabilisation des interventions effectuées et de produire un certain nombre d'états statistiques sur le suivi financier de la prestation ;

Considérant que les services du conseil général chargés de la gestion et du paiement de la prestation spécifique dépendance seront destinataires de ces informations, sous une forme nominative, pour ce qui concerne les bénéficiaires, mais anonyme s'agissant des intervenants ;

Considérant que les données nominatives concernant les bénéficiaires de la prestation spécifique dépendance et les prestations servies seront conservées par les services du conseil général pendant vingt-quatre mois après la fin du versement de la prestation ;

Considérant que les personnes âgées seront informées par le conseil général des modalités d'utilisation du dispositif : que leur droit d'accès et de rectification pourra s'exercer auprès du directeur des interventions sociales

et sanitaires du département des Bouches-du-Rhône : qu'en outre, lors de chaque intervention, elles pourront consulter, sur l'écran du lecteur, le temps effectué par l'intervenant ainsi que le nombre d'heures restant à effectuer : qu'enfin, elles recevront mensuellement un état récapitulatif des interventions effectuées qu'elles seront invitées à signer ;

Considérant qu'il appartiendra à chaque organisme prestataire d'informer ses salariés des modalités d'utilisation du dispositif et des conditions d'exercice de leur droit d'accès et de rectification ; qu'il est d'ores et déjà prévu que l'organisme prestataire remette à chaque intervenant un récapitulatif des interventions qu'il aura effectuées ;

Considérant que des mesures de sécurité adéquates ont été prises pour assurer la confidentialité des données échangées, notamment par l'utilisation de protocoles d'échanges sécurisés ;

Considérant que le conseil général des Bouches-du-Rhône devra porter à la connaissance de la Commission la liste des associations participant au dispositif ;

Émet un avis favorable au projet d'arrêté présenté par le président du conseil général des Bouches-du-Rhône concernant la mise en œuvre d'un traitement automatisé de données nominatives relatif à la gestion du suivi de la prestation spécifique dépendance dans le département, accordée à domicile.

III. « PIAF » OU LE TRAITEMENT DE L'AIDE SOCIALE FACULTATIVE À PARIS

Le Centre d'action sociale de la ville de Paris (CASVP), qui constitue le centre communal d'action sociale le plus important de France, a soumis pour avis à la CNIL une application de gestion de l'aide sociale facultative. L'élaboration de cet outil a été précédée d'une large concertation avec les futurs utilisateurs et la Commission elle-même. La structure particulière du CASVP en vingt sections en charge de l'attribution d'une trentaine de types d'aides financières facultatives et, par convention avec le département, des aides financières exceptionnelles au titre de l'aide sociale à l'enfance, a conduit le CASVP à concevoir une application différente de celles déjà mises en œuvre dans d'autres communes, puisqu'elle ne cumule pas la gestion de l'aide sociale légale et de son complément, l'aide sociale facultative.

En pratique, ce traitement dénommé « PIAF » est installé sur des postes de travail, situés dans les sections et les permanences d'accueil social, qui sont reliés à un serveur central sur lequel est implanté le fichier d'identification de tous les bénéficiaires des aides facultatives sur Paris. Cet annuaire enregistre les nom patronymique et marital, les prénoms, la date de naissance et l'adresse des bénéficiaires. Puisque le traitement permet de rapprocher les informations dont dispose chaque section, une personne ne devrait plus se trouver inscrite simultanément dans plusieurs sections d'arrondissements. À terme, il est prévu de

rendre accessible à partir des mêmes ordinateurs, l'application de gestion de l'aide sociale légale, afin qu'un même agent puisse instruire le dossier d'une personne qui vient solliciter, à la fois, une aide légale du département et une aide facultative de la mairie. Outre une fonctionnalité de renseignement des usagers sur l'attribution de prestations, le traitement « PIAF » permet d'optimiser la procédure d'instruction des dossiers, d'éditer des statistiques portant notamment, sur le nombre de personnes suivies, le nombre d'accords et de refus et certains croisements, par âge, par revenus, par catégorie d'aide ; enfin, il simplifie les opérations de comptabilisation et de mandatement et accélère les paiements.

Le traitement « PIAF » enregistre des informations concernant l'identification du demandeur et des membres du foyer, la nationalité (sous la forme : Française, Union européenne, autre), la situation familiale et professionnelle, les ressources et les charges ainsi que les références bancaires ou postales nécessaires pour le virement des prestations. À l'instar de la plupart des applications touchant à l'action sociale, une zone permettant la saisie d'un texte libre (commentaires, compte rendus ou observations) a été aménagée. À cet égard, et selon une doctrine désormais constante, la CNIL a tenu à rappeler que ces zones libres, souvent baptisées « vide-poche » ou encore « bloc-notes », ne doivent cependant contenir que des informations administratives nécessaires pour reconnaître ou écarter une demande, à l'exclusion de toute appréciation subjective, et a fortiori de toute donnée sensible au sens de l'article 31 de la loi du 6 janvier 1978 ; la commission a demandé que le projet d'acte réglementaire soit complété sur ce point.

Délibération n° 97-097 du 16 décembre 1997 portant avis sur la demande présentée par le Centre d'action sociale de la Ville de Paris concernant un traitement automatisé d'informations nominatives relatif à la gestion de l'aide sociale facultative, dénommé « Paris informatisation des aides facultatives » (PIAF)
(Demande d'avis n° 546 625)

La Commission nationale de l'informatique et des libertés,

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 loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu le décret n° 95-565 du 6 mai 1995 relatif au Centre d'action sociale de la Ville de Paris ;

Vu le règlement municipal portant conditions d'octroi des aides sociales facultatives ;

Vu le projet d'acte réglementaire présenté par le Centre d'action sociale de la Ville de Paris ;

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

Considérant que le Centre d'action sociale de la Ville de Paris a saisi la Commission d'une demande d'avis concernant la mise en œuvre, sur des moyens informatiques situés dans les sections d'arrondissements, les permanences sociales d'accueil et les services centraux du Centre, d'un traitement automatisé dont la finalité principale consiste à gérer les demandes d'attribution d'aides sociales facultatives, leur attribution et leur paiement ;

Considérant que les informations nominatives enregistrées sont relatives à l'identification des personnes sollicitant et bénéficiant des différentes prestations gérées par le Centre d'action sociale de la Ville de Paris, à leur nationalité (sous la forme Français, ressortissant de l'Union européenne, autre nationalité), à leur situation économique et financière, à leur vie professionnelle, à leur situation au regard du revenu minimum d'insertion et à leur numéro d'identification au RMI, à la composition du foyer, à leur adresse et aux références bancaires ou postales nécessaires au paiement des prestations ;

Considérant que ces informations sont pertinentes et non excessives au regard de la finalité du traitement ;

Considérant que le traitement dispose de zones de textes libres destinées à apporter des observations sur l'instruction du dossier de demande ou permettant de rédiger un compte rendu de visite : prend acte que toutes dispositions sont prises afin que n'y soient portées que des informations à caractère administratif destinées à apprécier l'ouverture du droit aux prestations et accessibles aux intéressés, à l'exclusion de toute appréciation subjective et de toute information relevant de l'article 31 de la loi du 6 janvier 1978 ; que l'acte réglementaire doit être complété afin d'indiquer que le traitement dispose d'une telle zone de texte libre ;

Considérant que les destinataires des informations sont, dans la limite de leurs attributions, les agents du Centre d'action sociale de la Ville de Paris, chargés, au sein de chaque section et permanence, de l'accueil et de l'instruction des dossiers et, au siège, des opérations de mandatement ou de paiement des allocations ; qu'au sein de chaque section ou permanence, les agents habilités n'ont accès qu'aux seuls dossiers du ressort de leur compétence : que, cependant, l'identité des bénéficiaires des aides sociales facultatives est consultable par les agents habilités des différentes sections afin d'éviter des inscriptions multiples dans plusieurs sections du Centre d'action sociale de la Ville de Paris ;

Considérant que les données nominatives sont conservées pendant une durée de deux ans après la date de fin d'effet de la dernière prestation accordée, sauf lorsque la personne concernée bénéficie de l'allocation de la Ville de Paris, les informations étant alors conservées pendant une durée de cinq ans : que cette durée n'est pas excessive au regard des conditions d'attribution de cette prestation financière qui disposent que le demandeur doit justifier d'une domiciliation sur Paris pendant trois ans sur une période de cinq ans précédant la demande ;

Considérant que toutes dispositions doivent être prises afin d'informer clairement les personnes concernées des droits qui leur sont offerts au titre de la loi du 6 janvier 1978 ; qu'ainsi il sera fait mention sur les demandes d'aides et sur les notifications de prestations des mentions prescrites par l'article 27 de la loi du 6 janvier 1978 ;

Considérant que le droit d'accès et de rectification, prévu en application des articles 34, 35 et 36 de la loi du 6 janvier 1978, s'exerce auprès du directeur de la section du Centre d'action sociale concernée ; Considérant que les mesures de sécurité prises pour assurer la confidentialité des données et l'accès différencié selon les habilitations des agents sont satisfaisantes ;

Émet un avis favorable au projet d'arrêté présenté par le Centre d'action sociale de la Ville de Paris concernant la mise en oeuvre d'un traitement automatisé de données nominatives relatif à la gestion de l'aide sociale facultative.

Chapitre 9

STATISTIQUES

I. L'UTILISATION DU FICHIER ELECTORAL DE L'INSEE

A. L'évaluation de la participation électorale

Après l'annonce de la dissolution de l'Assemblée nationale en 1997, l'INSEE a saisi la CNIL d'une demande d'avis concernant une étude sur la participation électorale aux prochains scrutins. Cette évaluation constitue en fait le prolongement de l'étude effectuée par l'INSEE à l'occasion des élections présidentielles et municipales de 1995 *[cf.* 16e rapport, p. 373).

L'INSEE a souhaité utiliser, pour l'étude de 1997, le même échantillon de communes et d'électeurs qu'en 1995, afin d'apprécier les comportements des électeurs au regard de l'abstention sur une longue période. Le traitement créé à l'époque avait concerné près de 40 000 électeurs sélectionnés dans le fichier des électeurs tenu par l'INSEE, soit environ 1500 personnes pour le ressort de chacune des vingt-deux directions régionales de l'INSEE.

Les agents de chaque direction régionale disposaient d'une liste des électeurs de l'échantillon, classés par commune d'inscription, afin de mentionner pour chaque électeur, après consultation des listes d'émargement, des informations sur leur participation électorale (a voté, n'a pas voté ou non trouvé sur la liste).

La Commission a tenu compte de ce que toutes les données utilisées pour réaliser cette étude provenaient soit de fichiers régulièrement déclarés à la CNIL, tel le fichier électoral, soit de documents accessibles au public telles les listes d'émargement, dont l'article L. 68 du code électoral précise qu'elles sont consultables par tout électeur durant les dix jours qui suivent un tour de scrutin.

Elle s'est par ailleurs intéressée aux publications de l'INSEE faisant apparaître, à la suite du traitement opéré en 1995, que seuls 11 % des électeurs n'avaient participé à aucun des 4 tours des scrutins réalisés en 1995.

Ces résultats démontraient l'intérêt pour l'INSEE de suivre en 1997 le comportement des électeurs sur lesquels avait porté l'enquête de 1995.

Ainsi, l'INSEE a fait part de son intention de poursuivre son étude sur l'itinéraire de participation électorale du même échantillon d'électeurs pendant l'année 1998, pour les élections régionales et les élections européennes ; le comportement de ces électeurs pourrait être analysé sur les cinq principales élections organisées en France. Dans cette perspective, l'INSEE a donc proposé de conserver sous forme nominative jusqu'en 1998 le fichier utilisé en 1997. Toutefois, la Commission a estimé que pour 1998 la demande était prématurée. Elle a donc limité en l'état son avis favorable aux élections de 1997.

Sollicitée à nouveau au début de l'année 1998, la Commission s'est prononcée favorablement à la prolongation de l'étude à l'occasion des scrutins régionaux. Elle a exigé que l'échantillon de personnes utilisé dans le cadre de cette étude soit détruit au terme de l'enquête (cf. délibération 98-016 du 3 mars 1998) afin qu'aucune identification des électeurs ne soit possible.

Délibération n° 97-046 du 10 juin 1997 portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives ayant pour objet la conduite d'une étude statistique sur l'évolution de la participation électorale en 1997
(Demande d'avis n° 368 533)

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 le code électoral ;

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistique ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié portant application de la loi du 6 janvier 1978 ;

Vu l'arrêté du 23 mai 1984 créant l'échantillon démographique permanent de l'INSEE ;

Vu l'arrêté du 25 novembre 1992 portant modification du traitement automatisé de gestion du fichier électoral ;

Vu l'arrêté du 12 avril 1995 portant création d'un traitement automatisé relatif à une étude statistique sur l'évolution de la participation électorale en 1995;

Vu le projet d'arrêté portant création d'un traitement automatisé relatif à une étude statistique sur l'évolution de la participation électorale en 1997 ;

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

Considérant que la CNIL est saisie, par l'INSEE d'une demande d'avis relative à une étude statistique sur la participation électorale de 40 000 électeurs aux différents scrutins de 1997 ;

Considérant que cette opération constitue le prolongement de l'étude statistique sur la participation électorale effectuée par l'INSEE en 1995 et créée par l'arrêté susvisé du 12 avril 1995 ;

Considérant que l'étude soumise à l'avis de la CNIL a pour objectif de rattacher individuellement aux électeurs de 1995 les comportements de participation de 1997 ;

Considérant que les 40 000 personnes seront sélectionnées dans le fichier électoral tenu par l'INSEE en fonction de leur appartenance à l'échantillon démographique permanent (EDP) ; que 2 000 personnes environ seront concernées dans chacune des vingt-deux directions régionales de l'INSEE ; que la sélection portera sur les mêmes communes qu'en 1995 et sur les électeurs ayant les mêmes dates de naissance ;

Considérant que dans un premier temps, la direction générale de l'INSEE confrontera la liste obtenue avec la base de données relative au répertoire des personnes physiques (BRPP) afin d'éliminer les électeurs décédés, radiés ou ayant perdu la nationalité française ; qu'un fichier de travail sera ainsi constitué qui comportera, pour chaque personne, le nom et les prénoms, le sexe, le numéro d'inscription au répertoire, la date de naissance, la commune d'inscription sur les listes électorales, un numéro d'ordre non signifiant ;

Considérant que dans un second temps, chaque direction régionale de l'INSEE sera destinataire, pour son ressort, d'une liste, par département, des électeurs de l'échantillon, classés par commune d'inscription ; que cette liste mentionnera le numéro d'ordre, le nom et les prénoms, le sexe, la date de naissance, la commune d'inscription en qualité d'électeur ;

Considérant que le numéro d'ordre doit permettre, lors des phases successives de l'enquête, de réunir les données relatives à la participation d'un même électeur aux différents scrutins de 1997 ;

Considérant qu'à partir de la consultation des listes d'émargement conformément aux dispositions de l'article L. 68 du code électoral, chaque direction régionale indiquera pour chaque intéressé : a voté, n'a pas voté ou non trouvé sur la liste ;

Considérant que, dans un délai de quinze jours après l'achèvement de la collecte, les données seront saisies dans un fichier de travail implanté au niveau de la direction régionale ; qu'une copie de ce fichier sera transmise à la direction générale de l'INSEE ;

Considérant que les documents papier ayant servi à la collecte seront détruits dès que cette transmission aura été effectuée ; que le fichier de travail sera conservé par la direction régionale jusqu'au dernier scrutin concerné par l'étude ;

Considérant que la direction générale procédera ensuite au regroupement des fichiers régionaux ; que le numéro d'ordre permettra grâce à une table de passage « numéro d'ordre — NIR » de rechercher dans l'échantillon démographique permanent les données suivantes : l'état matrimonial, le lieu de naissance, la taille de l'agglomération du domicile, le statut professionnel, le niveau de diplôme, la catégorie socioprofessionnelle ;

Considérant que, compte tenu de l'ensemble de ces données, ainsi que de sa commune d'inscription et de sa date de naissance, chaque électeur présente, sauf très rares exceptions, une « configuration singulière », qui permet un appariement entre le fichier de 1995 et celui de 1997 ; qu'il est ainsi possible de suivre la participation électorale des mêmes électeurs dans l'ensemble des scrutins présidentiels, municipaux et législatifs de 1995 et 1997 ; Considérant que chaque direction régionale sera destinataire d'un fichier comportant les données extraites de l'EDP mais ne comportant plus le numéro d'ordre, les nom et prénom ; qu'à partir de ce fichier, la direction régionale procédera à des exploitations locales ;

Considérant que le numéro d'ordre, les nom et prénoms seront également éliminés du fichier de travail de la direction générale dans le mois qui suit la validation des données relatives à la participation au dernier scrutin ;

Considérant que l'INSEE sera le seul destinataire des données recueillies ;
que ses travaux sont couverts par le secret statistique ;

Considérant que le droit d'accès prévu par l'article 34 de la loi du 6 janvier 1978 s'exercera auprès de la direction générale de l'INSEE ;

Émet un avis favorable au projet d'arrêté portant création du traitement.

B. La vérification des listes électorales de Guadeloupe

Les modalités d'utilisation du fichier électoral tenu par l'INSEE à des fins de vérification des listes électorales sont prévues par le code électoral qui autorise des échanges d'informations entre l'INSEE et les communes responsables de la tenue des listes électorales. A ce titre, les maires doivent informer l'INSEE de toute inscription ou radiation sur les listes ; de même, lorsque l'INSEE constate une irrégularité renouvelée ou prolongée dans les inscriptions (inscriptions sur deux listes, maintien de l'inscription d'une personne décédée ou privée de ses droits électoraux), la préfecture compétente doit en être avisée.

La préfecture de la Guadeloupe ayant signalé un écart important entre le nombre d'électeurs inscrits sur le fichier électoral tenu par l'INSEE et le nombre d'électeurs figurant sur les listes électorales des communes, le ministre de l'Intérieur a demandé à l'INSEE de procéder à plusieurs vérifications des listes électorales de la Guadeloupe, au regard de son propre fichier.

La CNIL a donné un avis favorable à l'application que l'INSEE a conçue pour mettre en évidence les divergences éventuelles pour chacune des communes du département de la Guadeloupe ; dans un souci de complète information, la Commission a souhaité que les maires concernés soient rendus destinataires des résultats de la comparaison dans la limite de ceux concernant leurs communes respectives.

Délibération n° 97-013 du 18 février 1997 portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives relatif au rapprochement des listes électorales de Guadeloupe avec le fichier électoral de l'INSEE

(Demande d'avis n° 496 735)

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 ;

Vu le code électoral ;

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 25 novembre 1992 du ministre de l'Économie et des Finances portant application du traitement automatisé de gestion du fichier électoral ;

Vu le projet d'arrêté, présenté par le ministre de l'Économie et des Finances, portant création du traitement ;

Après avoir entendu Madame Louise Cadoux, 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 oeuvre d'un traitement automatisé d'informations nominatives dont la finalité principale est le rapprochement des listes électorales de la Guadeloupe avec le fichier électoral géré par l'INSEE, conformément aux dispositions de l'article L. 37 du code électoral ;

Considérant que ce traitement est effectué à la demande du ministre de l'Intérieur dans un souci de vérification des listes électorales de la Guadeloupe ;

Considérant que le traitement automatisé permettra d'obtenir, pour chacune des communes du département de la Guadeloupe, d'une part un fichier des personnes inscrites sur les listes électorales avec l'indication des divergences avec le fichier électoral et d'autre part un fichier des personnes ne figurant pas sur les listes électorales de la commune mais apparaissant, au titre de la même commune, sur le fichier électoral ;

Considérant que les données traitées seront relatives au nom, prénom, sexe, date et lieu de naissance de chaque électeur ; qu'elles mentionneront sa qualité d'inscrit, radié, en incapacité électorale, décédé, non inscrit, la date d'inscription, de radiation ou de décès, l'origine de l'avis relatif à la situation actuelle ainsi que le motif de la radiation ;

Considérant que l'article 4 du projet d'arrêté prévoit que les informations individuelles sont communiquées, à titre exclusif, à la préfecture de Guadeloupe ; qu'il résulterait d'une telle rédaction que les maires des communes ne pourraient pas se voir communiquer les résultats nominatifs du traitement, pour leur commune ; que telle n'est pas l'intention du responsable du traitement ; qu'il y a donc lieu de modifier l'article 4 du projet d'acte afin

de préciser que les informations individuelles peuvent être communiquées au préfet et, chacun pour ce qui le concerne, aux maires des communes ;

Considérant que le droit d'accès prévu par l'article 34 de la loi n° 78-17 du 6 janvier 1978 s'exercera auprès de la préfecture de la Guadeloupe ;

Émet un avis favorable au projet d'arrêté portant création du traitement, sous réserve que l'article 4 soit ainsi rédigé « les informations individuelles énumérées à l'article 3 sont communiquées à la préfecture de la Guadeloupe et, chacun pour ce qui le concerne, aux maires des communes intéressées » ;

II. LE RECENSEMENT

A. Le recensement général de la population a Mayotte

La CNIL a examiné une demande de l'INSEE concernant le recensement général de la population (RGP) effectué à Mayotte en 1997.

Comme en métropole, les opérations de recensement dans les territoires d'outre-mer poursuivent un triple objectif :
- comptabiliser la population ;
- analyser les structures démographiques, professionnelles et les caractéristi ques du parc immobilier ;
- aider à la constitution d'une base d'échantillonnage de logements en vue des enquêtes statistiques ultérieures de l'INSEE.

Compte tenu de la spécificité de cette collectivité territoriale, certaines des données recueillies sont susceptibles de faire apparaître les opinions religieuses ou l'origine ethnique des personnes. Aussi, l'INSEE a-t-elle saisi la CNIL d'un projet de décret portant application de l'article 31 alinéa 3 de la loi du 6 janvier 1978.

Enfin, il convient de noter que les recommandations de la CNIL concernant la diffusion des données issues du RGP, telles qu'elles ont été définies à l'occasion du dernier recensement à Mayotte en 1991, ont été intégralement prises en compte. Ainsi, les données relatives au statut civil et à la polygamie ne seront disponibles qu'au niveau de la collectivité territoriale et aucun tableau statistique ne sera diffusé à un niveau inférieur à celui du village.

Délibération n° 97-027 du 1er avril 1997 portant avis favorable à la mise en œuvre, par l'INSEE, du recensement général de la population (RGP) à Mayotte

(Demande d'avis n° 505 596)

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 ;

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

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

Vu le projet de décret fixant la date et les conditions dans lesquelles sera exécuté le recensement général de la population à Mayotte ;

Vu le projet de décret portant application des dispositions de l'article 31 de la loi du 6 janvier 1978 au recensement général de la population à Mayotte ;

Vu le projet d'arrêté portant création d'un traitement automatisé réalisé à l'occasion du recensement général de la population à Mayotte ;

Après avoir entendu Monsieur Michel Bernard, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en sesobservations ;

Considérant que la Commission est saisie d'une demande d'avis concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour objet la collecte et l'exploitation de données dans le cadre du recensement général de la population dans la collectivité territoriale de Mayotte ;

Considérant que le recensement général de la population (RGP) à Mayotte sera effectué du 5 août au 2 septembre 1997, sous la responsabilité de l'Institut national de la statistique et des études économiques (INSEE) ;

Considérant que le recensement a pour finalité la détermination de la population légale de Mayotte, la production de statistiques permettant de décrire les structures socio-démographiques et les caractéristiques du parc immobilier et la constitution de bases d'échantillonnage de logements en vue des enquêtes statistiques ultérieures de l'INSEE ; que cette enquête a un caractère obligatoire ;

Considérant que les données collectées concerneront les personnes physiques, les logements et immeubles bâtis ; que les informations relatives aux personnes porteront sur le sexe, la date et le lieu de naissance, la nationalité, le statut civil (personnel ou de droit commun), la situation familiale avec l'indication de la polygamie, le niveau ou la nature de la formation, les activités professionnelles, les migrations, les conditions de logement ; Considérant qu'au regard des finalités poursuivies, ces catégories d'informations sont adéquates, pertinentes et non excessives ;

Considérant que les agents participant à la collecte et au traitement des données sont astreints au secret statistique en application des dispositions de la loi du 7 juin 1951 susvisée ;

Considérant que les destinataires des données seront l'INSEE et le service des Archives de France ; que l'archivage des documents et des fichiers du RGP fera l'objet d'un protocole d'accord entre le directeur général de l'INSEE et le directeur général des Archives de France ;

Considérant que les données statistiques issues du recensement ne pourront être cédées que sous forme de tableaux statistiques ;

Considérant que des tableaux détaillés seront disponibles au niveau de la collectivité territoriale, de la commune de Mamoudzou et de la Petite Terre ; que des tableaux standard pourront être obtenus au niveau des communes ; que des tableaux résumés seront disponibles au niveau des villages ;

Considérant que les tableaux comportant des données relatives à la polygamie et au statut civil ne pourront être disponibles qu'au niveau de la collectivité territoriale ;

Considérant que certains organismes publics énumérés à l'article 7, premier alinéa du projet d'acte réglementaire (les municipalités et syndicats de commune, les organismes d'aménagement du territoire, les organismes mettant en œuvre des politiques de la ville, les organismes publics effectuant des recherches scientifiques ou historiques et les organismes publics mettant en oeuvre des politiques sociales) pourront se voir céder des tableaux au niveau du district de recensement, sous réserve de la signature d'une convention de cession, dont le modèle a été approuvé par la Commission, signée entre l'INSEE et le bénéficiaire ;

Considérant que le droit d'accès prévu par l'article 34 de la loi du 6 janvier 1978, s'exercera auprès du préfet à Mayotte pendant les deux semaines suivant le dernier jour des opérations de collecte, puis passé ce délai auprès de la direction générale de l'INSEE à Paris ;

Émet un avis favorable au projet d'arrêté portant création d'un traitement automatisé à l'occasion du recensement général de la population à Mayotte.

Délibération n° 97-028 du 1er avril 1997 portant avis sur le projet de décret, présenté par l'INSEE, portant application des dispositions de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978, au traitement automatisé d'informations nominatives mis en œuvre à l'occasion du recensement général de la population (RGP) à Mayotte

(Demande d'avis n° 505 596)

La Commission nationale de l'informatique et des libertés ;

Vu l'article *75* de la Constitution ;

Vu le code pénal, notamment son article 725-5 ;

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 ;

Vu la loi n^{0} 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

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

Vu le projet de décret fixant la date et les conditions dans lesquelles sera exécuté le recensement général de la population à Mayotte ;

Vu le projet d'arrêté portant création d'un traitement automatisé réalisé à l'occasion du recensement général de la population à Mayotte ;

Vu le projet de décret portant application des dispositions de l'article 31 de la loi du 6 janvier 1978 au recensement général de la population à Mayotte ;

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

Considérant que la loi du 6 janvier 1978, dans son article 31, dispose qu'aucune donnée nominative faisant apparaître directement ou indirectement les origines raciales, ou les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales ou les mœurs des personnes, ne peut être mise ou conservée en mémoire informatique, sauf accord exprès des intéressés ;

Considérant que l'alinéa 3 de l'article précité prévoit qu'il peut être fait exception à cette interdiction pour des motifs d'intérêt public, sur proposition ou avis conforme de la Commission par décret en Conseil d'État ; Considérant que parmi les données collectées lors du recensement à Mayotte, figureront la polygamie et le statut civil des personnes ; que ces données sont susceptibles de faire apparaître l'origine ethnique et les opinions religieuses des personnes interrogées ;

Considérant que la Commission est saisie par le ministre de l'Économie et des Finances d'un projet de décret portant application au traitement du RGP des dispositions de l'article 31 alinéa 3 précité ;

Considérant que la collecte de l'information relative à la polygamie et au statut civil des personnes, compte tenu des caractéristiques socio-démographiques et du régime juridique propres à la collectivité territoriale de Mayotte, répond à un motif d'intérêt public, au sens de l'alinéa 3 de l'article 31 précité ;

Émet un avis conforme au projet de décret portant application des dispositions de l'article 31 de la loi du 6 janvier 1978 au recensement général de la population à Mayotte.

B. L'enquête « famille » à la Réunion

Depuis plus de quarante ans, l'INSEE associe au recensement général de la population réalisé en métropole une enquête dite « famille », traditionnellement effectuée dans un district de recensement sur cinquante, et qui doit permettre d'analyser certains comportements démographiques. En revanche, c'est la première fois que les pouvoirs publics ont prévu de réaliser une telle enquête dans un département d'outre-mer, en l'espèce l'île de la Réunion, de novembre à décembre 1997. Il s'agissait tout particulièrement d'étudier l'évolution de la structure familiale au regard d'une croissance de la population quatre fois plus élevée qu'en métropole.

Bien que l'enquête ait pu donner lieu à une simple déclaration en référence à la norme simplifiée n° 19, eu égard à son caractère facultatif, l'INSEE a néanmoins saisi la CNIL d'une demande d'avis en application de

l'article 15 de la loi du 6 janvier 1978, et ce dans le souci d'adopter la même procédure que celle utilisée pour la déclaration de l'enquête « famille » en métropole (cf. 17e rapport, p. 400).

L'enquête « famille » effectuée à la Réunion doit concerner 4500 ménages, comportant une femme âgée de 15 à 64 ans, l'échantillon étant tiré au sort. La Commission a relevé, non sans émettre quelques réserves, que le questionnaire élaboré pour cette enquête touchait de très près à l'intimité de la vie privée. Compte tenu de son objet, l'enquête portait en effet, notamment, sur le statut des enfants de la personne interrogée (biologique ou adopté) et les grossesses (contexte, suivi médical, allaitement et mode de garde de l'enfant), d'autres questions devaient permettre d'apprécier si un lien entre pratique religieuse et pratique contraceptive pouvait ou non être établi. Aussi, malgré l'assurance donnée que les enquêteurs seraient sensibilisés aux problèmes de confidentialité, la Commission a-t-elle estimé qu'il convenait que soit rappelé oralement, au début de l'entretien le caractère facultatif de l'enquête qui était par ailleurs indiqué sur le courrier adressé aux personnes appelées à y participer.

Toutefois, la Commission a relevé que les noms, prénoms et adresses n'étant pas saisis informatiquement, les personnes concernées ne pourraient, de ce fait, exercer leur droit d'accès auprès de la direction régionale de l'INSEE à la Réunion que durant trois mois, durée pendant laquelle l'enquêteur conserve un « carnet de tournée » permettant de relier l'adresse du demandeur à l'identifiant du logement utilisé pour l'enquête.

La CNIL a donné un avis favorable à la mise en œuvre du traitement de données nominatives connexe à l'enquête « famille » à la Réunion en demandant à être destinataire des instructions qui seraient données aux agents enquêteurs.

Délibération n° 97-079 du 21 octobre 1997 portant avis favorable, à la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête famille effectuée à la Réunion

(Demande d'avis n° 532 664)

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, notamment ses articles 15 et 27 ;

Vu la loi n0 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu le décret n° 78-774 du 17 juillet 1978 portant application de la loi susvisée de 1978 ;

Vu le projet d'arrêté portant création du traitement présenté par le directeur général de l'INSEE ;

Après avoir entendu Monsieur Charles Renard, 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, de la mise en oeuvre d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête famille qui doit être réalisée, pour la première fois, dans l'île de la Réunion ; que cette enquête a pour objet d'étudier l'évolution du modèle familial et de la fécondité ;

Considérant que la collecte de données aura lieu de novembre à décembre 1997 auprès de 4500 ménages ; que dans chaque ménage, une femme âgée de 15 à 64 ans sera tirée au sort pour répondre aux questions posées par l'agent enquêteur ;

Considérant que les données recueillies seront relatives à la composition du ménage : lien avec le chef de ménage, âge, sexe, éducation, survie et résidence des parents pour les personnes de moins de 15 ans, état matrimonial ; qu'en ce qui concerne la personne interrogée, les informations concerneront les enfants biologiques et adoptés, les grossesses postérieures à 1990 (contexte de la grossesse, suivi médical, allaitement, mode de garde de l'enfant), la description des autres enfants vivant ou ayant vécu au foyer de cette personne, la situation personnelle (profession, éducation, lien à la religion, maîtrise de l'écrit) et les interruptions d'activité pour élever les enfants, la description des différentes périodes de la vie de couple, la planification des naissances, la connaissance et la pratique de la contraception, la stérilisation, les intentions de fécondité, la situation de la génération précédente, les migrations de la personne interrogée et de ses enfants ; Considérant que les données seront, lors de la collecte, saisies sur microportable ; que les nom, prénom et adresse des personnes enquêtées ne seront pas enregistrés dans le traitement ;

Considérant que cette enquête aura un caractère facultatif ; que de surcroît, les personnes disposeront de la faculté de ne pas répondre à certaines questions touchant directement à l'intimité de leur vie privée ;

Considérant qu'il convient que le courrier qui sera adressé aux personnes figurant dans l'échantillon rappelle le caractère facultatif de l'enquête et souligne, s'agissant des questions qui relèvent le plus directement de l'intimité de la vie privée, que les personnes interrogées auront la faculté de refuser d'y répondre ; que cette faculté soit rappelée oralement au début de l'entretien ;

Considérant de surcroît, compte tenu de la nature de l'enquête, et s'agissant des résidents actuels et des visiteurs de la personne interrogée qu'il y a lieu de prévoir que seul le prénom sera collecté à l'exclusion du nom ;

Considérant que les destinataires des données recueillies seront les seuls agents habilités de l'INSEE et de l'INED ;

Considérant que les personnes interrogées pourront exercer le droit d'accès qui leur est reconnu par la loi du 6 janvier 1978, auprès de la direction régionale de l'INSEE à la Réunion, pendant un délai de trois mois à compter de la date de l'entretien ;

Émet un avis favorable au projet d'arrêté portant création du traitement qui lui est soumis.

Demande à être destinataire des instructions données aux agents enquêteurs.

III. L'ENQUETE SUR LES REVENUS DES MÉNAGES EN 1996

Le ministère de l'Economie et des Finances a déclaré à la CNIL, en référence à la norme simplifiée n° 26 concernant les traitements à caractère statistique effectués par les services producteurs d'informations statistiques, la mise en œuvre par l'INSEE d'une étude sur les revenus des ménages déclarés à l'administration fiscale en 1996. Cette enquête doit permettre d'apprécier le comportement économique des ménages, notamment dans les périodes de chômage ou d'activité partielle. L'examen des déclarations de revenus reçues par la direction générale des impôts (DGI), l'analyse de la distribution des revenus et de son évolution, ainsi que l'étude de la composition des revenus des ménages en fonction de divers critères (âge, catégorie socioprofessionnelle, structure familiale) constituent les bases de cette enquête. Sa réalisation suppose donc de pouvoir regrouper l'ensemble des revenus déclarés par les différents foyers fiscaux composant un même ménage, c'est-à-dire les personnes domiciliées dans un même logement.

Toutefois, lors d'un premier examen en séance plénière, la CNIL a d'emblée exprimé de fortes réserves sur le fait que le dispositif de collecte des informations portées sur les déclarations de revenus des contribuables directement par les agents de la DGI, qui sont par ailleurs chargés du contrôle de la situation fiscale des mêmes ménages, ne paraissait pas de nature à garantir le respect de l'article L. 84 du livre des procédures fiscales selon lequel « les renseignements... recueillis au cours des enquêtes statistiques... ne peuvent en aucun cas être utilisés à des fins de contrôle fiscal ». Elle conduisait en effet à communiquer à ces agents les informations recueillies par l'INSEE sur la composition des ménages.

Aussi, la Commission a-t-elle proposé à l'INSEE d'expérimenter une informatisation complète des opérations de collecte des informations fiscales, sur le base d'un transfert à l'INSEE de données détenues par l'administration fiscale, de sorte que les agents de l'INSEE puissent retrouver eux-mêmes les foyers fiscaux concernés et ne communiquer, en retour, aux services informatiques de la DGI, que des numéros correspondants à leurs dossiers. Cette solution, qui revêt l'avantage d'éviter d'avoir à transmettre à l'administration fiscale des données collectées par l'INSEE auprès des contribuables, est conforme à la loi du 23 décembre 1986, qui offre à l'INSEE la possibilité d'être destinataire de l'ensemble des informations nominatives conservées dans les fichiers détenus par une administration, une collectivité locale, ou un organisme gérant un service public, à l'exclusion des données relatives à la santé ou à la vie sexuelle.

À l'issue de cette expérimentation qui, démontrant son efficacité, a satisfait toutes les parties, la CNIL a délivré un récépissé de déclaration de conformité à la norme n° 26 d'un nouveau projet de traitement respectant ses préconisations pour garantir le secret statistique.

Délibération n° 97-077 du 7 octobre 1997 concernant une déclaration simplifiée du ministère de l'Économie et des Finances relative à la réalisation d'une enquête de l'INSEE sur les revenus des ménages en 1996 à partir de l'exploitation des déclarations de revenus

(Déclaration simplifiée n° 465 878)

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° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques, notamment son article 7 bis ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ;

Vu l'article L. 84 du Livre des procédures fiscales ;

Vu l'arrêté du 5 janvier 1990 du ministre en charge du Budget, modifiant l'arrêté relatif à la création d'un système automatisé de gestion de l'identité et des adresses des contribuables à l'impôt sur le revenu et à la taxe d'habitation (fichier « FIP ») ;

Vu la délibération n° 84-38 du 13 novembre 1984 portant création de la norme simplifiée n° 26 relative aux traitements à caractère statistique effectués, à partir de documents ou de fichiers de gestion contenant des informations nominatives sur des personnes physiques, par les services producteurs d'informations statistiques au sens au décret du 17 juillet 1984 ;

Vu la déclaration simplifiée n° 465 878 présentée par le ministère de l'Économie et des Finances ;

Après avoir entendu Messieurs Thierry Cathala et Charles Renard en leur rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Considérant que le ministère de l'Économie et des Finances a saisi la Commission d'une déclaration simplifiée se référant à la norme simplifiée n° 26, qui concerne la mise en œuvre par l'INSEE d'une étude sur les revenus des ménages déclarés en 1996 à l'administration fiscale; que l'objet de cette étude est d'analyser la distribution et la composition des revenus des ménages, considérés en tant qu'unités économiques au sein desquelles les ressources sont mises en commun ;

Considérant que l'étude porte sur 25 000 ménages appartenant déjà à l'échantillon de population suivi au titre de l'enquête « Emploi » de l'INSEE, dans le but de rapprocher les revenus déclarés à la direction générale des impôts (DGI) par les ménages des conditions d'activité de leurs membres et ainsi d'évaluer les conséquences sur les revenus des périodes de chômage ou d'activité à temps partiel ;

Considérant que l'INSEE et la DGI avaient initialement envisagé de transmettre aux centres des impôts (CDI) la structure des ménages de l'échantillon telle qu'elle avait été communiquée à l'INSEE par les personnes enquêtées ;

que ce dispositif n'était pas de nature à garantir le respect de l'article L. 84 du Livre des procédures fiscales qui exclut que les données nominatives recueillies au cours d'une enquête statistique puissent être utilisées à des fins de contrôle fiscal ; que les deux administrations du ministère de l'Économie et des Finances ont finalement proposé que la collecte des informations fiscales soit dorénavant entièrement automatisée, en excluant totalement le concours des agents des CDI ;

Considérant que, dans ce nouveau dispositif, la DGI communiquera dans un premier temps à l'INSEE le fichier « FIP » qui recense, pour chaque direction des services fiscaux, les foyers fiscaux assujettis à l'impôt sur le revenu, la taxe d'habitation et l'impôt de solidarité sur la fortune et leur attribue un « numéro FIP » ; que l'appariement du fichier « FIP » avec une partie du fichier de l'enquête « Emploi » permettra aux agents de l'INSEE d'obtenir le « numéro FIP » des foyers fiscaux qui font partie de l'échantillon retenu, afin de transmettre cette seule information aux centres informatiques de la DGI, à l'exclusion de tout renseignement recueilli par l'INSEE auprès des contribuables ;

Considérant que le fichier des « numéros FIP » des foyers fiscaux ainsi sélectionnés sera rapproché, dans un second temps, du fichier « POTE » de la DGI, qui comporte les éléments de taxation portés sur les déclarations de revenus et le montant de l'impôt sur le revenu, ainsi que du traitement « TH », où figure le montant de la taxe d'habitation ;

Considérant que cette méthode présente les garanties adéquates au regard du secret statistique ; qu'en outre, son expérimentation, qui a été menée par l'INSEE et la DGI dans le département du Rhône, a permis de vérifier l'efficacité du système proposé ;

Est d'avis que le récépissé de déclaration de conformité à la norme simplifiée n° 26 doit être délivré au ministère de l'Economie et des Finances.

IV. L'EXPLOITATION STATISTIQUE DES PERMIS DE CONSTRUIRE

La direction des affaires économiques et internationales du ministère de l'Équipement, du Logement, des Transports et du Tourisme a adressé à la CNIL une demande d'avis relative à un traitement dénommé « SITADEL » dont la finalité principale est la collecte et la diffusion de données statistiques sur la construction neuve.

Cette nouvelle application bâtie sur l'utilisation des informations issues de l'instruction des permis de construire tend en réalité à se substituer aux traitements précédemment exploités sous la dénomination « SIROCO » (1980), puis « SICLONE » (1993), dont semblent résulter des opérations pouvant poser problème au regard de la protection des données personnelles et qui en tout état de cause, ont suscité des réclamations auprès de la CNIL.

En effet, depuis 1980, les coordonnées des personnes qui déposent en mairie une demande de permis de construire sont transmises à « tout demandeu

public ou privé dans le cadre d'études statistiques ou d'opérations commerciales ». Ces opérations étaient réalisées jusqu'alors dans la plus grande opacité vis-à-vis des intéressés, puisqu'ils n'en étaient pas spécifiquement informés, et ne pouvaient dès lors pas exercer leur droit d'opposition. En pratique, cette cession des données à des fins commerciales s'effectue tant au niveau des directions régionales que du ministère de l'Équipement.

À l'issue d'une concertation avec le ministre de l'Équipement, le fonctionnement du fichier « SITADEL » a été très sensiblement amélioré. En effet, le ministère s'est engagé à modifier les formulaires de demande de permis de construire de sorte qu'une mention spécifique informe les demandeurs de leur droit d'opposition à la communication des informations à des sociétés publiques ou privées à des fins commerciales et à adresser aux maires une circulaire leur demandant de porter cette information à la connaissance des personnes déposant une demande d'autorisation de construire.

La mention d'information, élaborée en concertation avec la CNIL, est la suivante : « La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, s'applique aux réponses contenues dans ce formulaire pour les personnes physiques. Elle garantit un droit d'accès et de rectification pour les données les concernant qui peut être exercé auprès de la mairie du lieu des travaux. Le droit d'opposition à toute cession visant à permettre une utilisation de ces informations à des fins commerciales peut s'exercer auprès de la mairie, de la direction départementale de l'équipement ou de la direction régionale de l'équipement du lieu des travaux ».

La Commission se félicite de ce progrès qui, tout en assurant le respect des dispositions actuelles relatives à la protection des données, va dans le sens préconisé par la directive européenne, dont l'article 14 prévoit que toute personne puisse s'opposer, sur demande et gratuitement, au traitement à des fins commerciales des données la concernant ou soit informée de ses droits préalablement à la première communication ou utilisation à des fins commerciales de ces données.

Chapitre 10

TRAVAIL ET EMPLOI

I. LE « FICHIER HISTORIQUE » DE L'ANPE

L'ANPE a saisi la CNIL d'un projet de création d'un fichier statistique dénommé «fichier historique» dont la vocation est de mieux appréhender l'impact des mesures prises en faveur de l'emploi. À cet effet, et c'est une nouveauté, l'ANPE se propose de constituer ce fichier de références, dont l'unité statistique de base serait, non plus la demande d'emploi, c'est-à-dire une formalité administrative, mais le demandeur d'emploi. Le « fichier historique » constitue donc un instrument d'analyse de la population inscrite comme demandeur d'emploi, ce traitement permettant d'enregistrer les périodes travaillées et chômées d'une même personne. D'abord conçu comme un outil d'évaluation de l'impact des mesures pour l'emploi et des prestations fournies par l'ANPE, le « fichier historique » devrait aussi permettre de faire l'économie d'enquêtes ponctuelles et coûteuses sur le devenir des demandeurs d'emplois, notamment l'enquête baptisée « trajectoire des demandeurs d'emplois » qui est effectuée depuis 1995 tous les six mois.

Le « fichier historique » est constitué à partir de l'application de gestion de la demande d'emploi « Gide 1 Bis », commune à l'ANPE et aux ASSEDIC (cf. 16^{e} rapport, p. 351). Le « fichier historique » devrait donc recenser tous les événements concernant les personnes inscrites comme demandeurs d'emploi à partir du 1er juillet 1993 et les conserver pendant trente-sept mois après la fin de la période de chômage. À cette fin, sont enregistrées : le numéro d'identification interne ANPE/ASSEDIC, qui peut le cas échéant être lié à une personne identifiable, le sexe, l'année et le mois de naissance, la commune de résidence, le canton de résidence, la nationalité, le nombre d'enfants à charge, la situation

de famille, le niveau de formation atteint, le secteur de formation, le diplôme obtenu, les besoins de formation.

Les destinataires naturels de ce fichier sous sa forme nationale sont les services de la direction générale de l'ANPE. Les agences locales pour l'emploi ne sont destinataires que d'informations réduites et agrégées sous forme de tableau, en particulier d'informations liées à leur bassin d'emploi. Les services statistiques ministériels, en particulier le ministère de l'Emploi et l'INSEE, souhaitaient avoir accès aux informations issues du fichier historique dans un but d'étude. Il a donc été prévu par la CNIL, en concertation avec l'ANPE, que lorsque des partenaires institutionnels de l'ANPE souhaiteraient avoir accès à ces informations, des conventions précises et limitées en définissant le cadre seraient conclues, conventions prévoyant notamment la forme des formalités préalables à accomplir auprès de la Commission.

Outre l'information des demandeurs d'emplois de sa mise en œuvre de ce « fichier historique » par voie d'affichage, la CNIL a demandé une information individuelle des personnes et, dans ces conditions, a émis un avis favorable à ce projet de l'ANPE.

Délibération n° 97-080 du 21 octobre 1997 portant avis sur un traitement automatisé d'informations nominatives présenté par l'ANPE dénommé « fichier historique » et ayant pour finalité l'amélioration de la connaissance des demandeurs d'emplois et de la demande d'emploi

(Demande d'avis n° 511 632)

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 code du travail et notamment les articles L. 311.7 et R. 311.4.4 ;

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

Vu la délibération n° 96-107 du 17 décembre 1996 ;

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

Considérant que l'ANPE a déposé un dossier de demande d'avis concernant la constitution d'un fichier statistique dénommé « fichier historique » devant permettre de mieux appréhender la demande d'emploi, ainsi que l'impact des politiques de l'emploi sur la demande d'emploi ;

Considérant que désormais ce sera le demandeur d'emploi qui constituera l'unité statistique de référence et non plus la demande d'emploi ;

Considérant que le fichier historique est constitué à partir du fichier Gide 1 Bis commun à l'ANPE et aux ASSEDIC ;

Considérant que le fichier projeté est dit « historique » car il est destiné à enregistrer tous les événements successifs concernant les personnes inscrites comme demandeurs d'emplois à partir du premier juillet 1993 ;

Considérant que le fichier doit permettre l'analyse de la population inscrite comme demandeur d'emploi afin d'éviter certaines enquêtes de panel destinées à analyser les trajectoires des demandeurs d'emplois; que le fichier doit également constituer un outil d'évaluation, afin d'évaluer l'impact des mesures pour l'emploi et des prestations fournies par l'agence ; que le fichier doit permettre enfin des simulations offrant la possibilité d'anticiper les résultats de scénarios d'action pour la formation ou l'emploi ; Considérant que les données enregistrées dans le fichier historique concernant les demandeurs d'emplois sont le numéro d'identification interne ANPE/ASSEDIC, le sexe, l'année et le mois de naissance, la commune de résidence, le canton de résidence, la nationalité, le nombre d'enfants à charge, la situation de famille, le niveau de formation atteint, le secteur de formation, le diplôme obtenu, les besoins de formations ; qu'il y a lieu de souligner que ne sont pas enregistrés ni le nom, ni le prénom, ni l'adresse de la personne concernée ;

Considérant que s'agissant de la vie professionnelle, sont enregistrés le numéro de l'agence locale de rattachement, la date et le mode d'inscription, le motif, le numéro de ROME dominant, la durée d'expérience, le type de contrat recherché, la durée hebdomadaire souhaitée, la disponibilité, la situation au regard de l'emploi, les dates d'annulations, de péremption de la demande, le nombre d'heures d'activité réduite, la nature de la période, le mois de la période, la date et le type d'entretien, l'unité prestataire, le type de prestation, l'organisme, le type, la date et le contenu de plan de formation, le nombre de stage, l'entrée effective en formation, les dates de début et de fin de stage, la catégorie d'organisme, la durée totale de la formation, la catégorie de financement, la durée hebdomadaire, le coût horaire, la participation au coût, l'éligibilité au Fond social européen ;

Considérant que la situation économique telle que la perception du RMI et le type d'indemnisation sont également enregistrés ; Considérant que toutes les informations sont conservées pendant une période prenant fin trente-sept mois après la fin de la période de chômage et l'annulation de la demande d'emploi qui en découle ; qu'ainsi un demandeur d'emploi qui connaîtrait des périodes d'embauche ou d'inactivité d'une durée inférieure à trois ans serait maintenu dans le fichier aussi longtemps qu'il n'aurait pas retrouvé un emploi d'une durée supérieure à trois ans ; Considérant que cette durée de conservation est justifiée par les finalités du traitement ;

Considérant que les destinataires des informations sont exclusivement les services de la direction générale de l'ANPE ; que les directions régionales, les directions départementales et les agences locales de l'ANPE n'auront accès qu'aux formes réduites et agrégées des variables du fichier historique ; Considérant que l'ANPE envisage de conclure des conventions de partenariat avec des partenaires institutionnels (DARES, INSEE, services statistiques des ministères et les laboratoires de recherche relevant du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche) ; Considérant que ces partenaires de l'ANPE sont destinataires d'informations indirectement nominatives au même titre que la direction générale de

l'ANPE ; que ces partenaires pourront être destinataires soit des données brutes, soit des indicateurs statistiques fournis par l'ANPE ; Considérant que l'INSEE et les laboratoires et centres de recherche relevant du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche possédant la qualité de service statistiques ministériels ont vocation à traiter ces données statistiques ; que l'article 7 bis de la loi du 7 juin 1951 prévoit que l'INSEE peut être destinataire à des fins exclusivement statistiques de données concernant des personnes physiques collectées par des établissements publics ;

Considérant qu'une convention a été passée entre la DARES et l'ANPE relative à la production et à la diffusion de nouvelles statistiques du marché du travail destinées à remplacer celles qui sont actuellement produites ; que ces nouvelles statistiques préciseront le stock de demandeurs d'emplois en fin de mois ainsi que les flux d'entrées et de sorties ;

Considérant que l'ANPE a prévu que des conventions d'étude pourraient être passées avec les différents partenaires précisant l'objet de la convention, les modalités d'exécution, le calendrier, le personnel chargé de l'étude, la durée de la convention ;

Considérant qu'une clause type de confidentialité sera adoptée suivant les partenaires concernés ; que cette clause devra préciser notamment l'obligation pour le partenaire de respecter la loi du 6 janvier 1978 dans le cas où les données transmises feraient l'objet d'un traitement automatisé d'informations nominatives ou indirectement nominatives ;

Considérant qu'il y a lieu en tout état de cause de prévoir dans ces conventions qu'en cas de diffusion de tableaux statistiques, les cases concernant moins de cinq personnes seront blanchies ; Considérant que les demandeurs d'emplois seront informés de la mise en œuvre de ce traitement par l'affichage d'une note dans l'agence locale pour l'emploi et chez les partenaires habilités de niveau 3 ayant signé une convention avec l'agence au sens de la délibération n° 96-107 du 17 décembre 1996 ; que cette note précisera que les informations recueillies font l'objet d'un traitement opérationnel, Gide 1 bis, et d'un traitement statistique à partir d'un enregistrement dans le fichier historique ainsi que les destinataires des informations ;

Considérant que les mesures de sécurités mises en oeuvres sont satisfasantes ; que ces sécurités reposent notamment sur des systèmes de mots de passe, propre à chaque utilisateur et à chaque application ; Demande, nonobstant l'affichage de la note d'information dans les agences locales pour l'emploi et chez les partenaires habilités de niveau 3 précités, que les demandeurs d'emplois fassent l'objet d'une information individualisée reprenant les fermes de la note précitée ;
Émet un avis favorable au projet de décision présenté par le conseil d'administration de l'ANPE.

II. LE CONTROLE DES SALARIES

De plus en plus d'entreprises disposent de moyens techniques leur permettant d'assurer un suivi instantané de l'activité de leurs salariés : badges, caméras, autocommutateurs, surveillance du réseau informatique... Aussi la Commission est-elle depuis plusieurs années saisie par des salariés qui se sentent surveillés dans leurs moindre gestes ou déplacements.

A. Les points du permis de conduire et le recrutement

En 1997, l'attention de la CNIL a été appelée sur le fait que certains questionnaires de recrutement comportent une question sur le nombre de points dont le candidat à l'emploi dispose sur son permis de conduire. En effet, plusieurs entreprises, employant de nombreux conducteurs ou des agents commerciaux dont l'outil de travail quotidien est un véhicule, ont déposé à la Commission des dossiers de déclaration prévoyant la collecte du, nombre de points figurant sur le permis de conduire des candidats à un poste. Ces sociétés font généralement valoir que cette information leur est nécessaire pour juger de l'aptitude professionnelle de la personne à occuper l'emploi proposé et que la perte de validité du permis entraînerait le licenciement de la personne ou sa mise à pied.

La loi du 10 juillet 1989 relative à diverses dispositions en matière de sécurité routière et de contraventions a en effet instauré un permis de conduire à points, dont le nombre, fixé à douze, est réduit de plein droit si son titulaire commet certaines infractions liées à la conduite d'un véhicule (excès de vitesse, état d'ivresse, homicide..). Lorsque le nombre de points devient nul, le permis perd sa validité, un nouveau permis de conduire ne pouvant être sollicité avant six mois.

Les entreprises ignorent généralement que le souci de renforcer la sécurité routière ne doit pas entraîner de préjudice social pour les personnes, en particulier au regard de la situation de l'emploi ou de la chance d'insertion professionnelle. C'est pourquoi le législateur a prévu que seules les autorités administratives et judiciaires pouvaient avoir accès aux informations relatives aux nombre de points, « à l'exclusion des employeurs, assureurs et toutes autres personnes physiques ou morales » (article L 11.6 du code de la route). La crainte que ces dispositions légales ne soient détournées a d'ailleurs conduit à prévoir que si une personne exerce son droit d'accès et de rectification aux informations figurant dans le fichier des permis de conduire, aucun relevé ne peut lui être délivré, précisément pour que l'on n'exige pas d'elle, dans des circonstances étrangères aux préoccupations de la police de la circulation, la production de son relevé de points. Ainsi, la CNIL rappelle-t-elle aux employeurs les règles, encore souvent ignorées, applicables en la matière.

B. La mesure de la productivité des salariés

Depuis plusieurs années, la CNIL est très attentive aux différentes formes de contrôle des salariés dans l'entreprise, que le recours aux nouvelles technologies renforce incontestablement. Le téléphone constitue une pièce maîtresse de cette surveillance d'un nouveau type. Dès 1984, la CNIL avait adopté une recommandation relative aux autocommutateurs téléphoniques sur les lieux de travail (cf. 5e rapport, p. 109 et 242). Par la suite, l'essor des autocommutateurs, essentiellement destinés à la facturation des appels, a conduit la CNIL à adopter deux normes simplifiées destinées à mieux encadrer leur utilisation et à inciter les personnes qui mettent en œuvre ces systèmes à les déclarer (*cf.* 15e rapport, p. *75).*

Cependant, la Commission est désormais saisie de déclarations de mise en œuvre de systèmes plus sophistiqués, dont la finalité est d'enregistrer des conversations téléphoniques : en cas d'appel d'urgence (appels depuis des ascenseurs lors d'incidents, appels depuis les bornes d'urgences sur les bords des autoroutes) ou encore à des fins de formation et de contrôle de la qualité des prestations téléphoniques.

Une société spécialisée dans la vente directe de produits d'assurance a déclaré un système téléphonique destiné à superviser les chargés de clientèle et à procéder à un « contrôle-qualité » par le moyen d'écoutes et d'enregistrement des conversations téléphoniques avec la clientèle.

Ainsi, outre les fonctions traditionnelles d'accueil et de répartition des appels d'un autocommutateur, il s'agit également d'effectuer l'analyse quantitative et qualitative des appels téléphoniques entrants et sortants. À cet effet, les informations concernant l'usage du poste téléphonique par les agents commerciaux chargés de clientèle (numéro du poste, nom de la personne, temps passé en réception d'appel, temps passé en émission d'appel, temps de présence sur le poste, nombre de communications arrivées sur le poste, nombre de communications parties du poste, nombre d'appels non décrochés, heures de début et de fin d'observation), ainsi que des informations propres à chaque appel téléphonique (mise en attente, renvoi de poste...) sont enregistrées ; le traitement de l'ensemble de ces informations permet d'apprécier la qualité du service rendu, de connaître le temps de réaction des consommateurs aux campagnes publicitaires, leurs effets selon le média utilisé et d'adapter les campagnes en fonction des résultats obtenus.

Enfin, les conversations téléphoniques peuvent être écoutées et enregistrées pour assurer l'encadrement opérationnel et technique des chargés de clientèle ; dans le souci d'apprécier la qualité de l'entretien téléphonique, d'améliorer la formation continue des opérateurs et de « prévenir le risque de communication d'informations erronées à la clientèle ». Les conversations captées sont le plus souvent numérisées, stockées et répertoriées avec le numéro de poste et le nom du salarié ; pour autant, les enregistrements ne peuvent être utilisés à titre de preuve contre un salarié.

La CNIL veille à ce que de tels dispositifs soient conformes aux prescriptions de la loi du 6 janvier 1978 et aux dispositions du code pénal. Aussi recommande-t-elle de manière générale que :
- les salariés soient informés de l'existence d'un système préalablement à sa mise en place, des conséquences individuelles qui pourront en découler et des périodes pendant lesquelles leurs conversations seront enregistrées ;
- les salariés disposent de lignes téléphoniques non connectées au dispositif d'écoute et ce, notamment, pour leurs conversations passées à titre privé ;
- les salariés aient connaissance du compte rendu de la conversation enregis trée et puissent formuler d'éventuelles observations ;
- les enregistrements des conversations, alors qu'il s'agit d'opérer des contrôles de la qualité du service téléphonique rendu, ne soient conservés que le temps strictement nécessaire à l'objectif poursuivi, notamment que la bande soit effacée dès qu'elle a été écoutée.

En l'espèce, la société concernée a prévu aussi que les personnes concernées seraient informées que les lignes de service, séparées des lignes téléphoniques réservées aux appels internes et personnels, peuvent être, à tout moment, enregistrées ou écoutées ; et en pratique, le lendemain d'un enregistrement, elles sont avisées que l'écoute a eu lieu. Une exploitation de l'enregistrement peut être réalisée dans les 48 heures qui suivent, 72 heures si l'enregistrement a eu lieu un vendredi ou veille de jour férié, ces durées étant des durées maximales de conservation des informations.

En revanche, le problème demeure posé de l'information des clients qui dans la plupart des cas sont dans l'ignorance de l'éventualité d'une écoute. Sur ce point l'information des clients peut être faite par tous moyens utiles, comme l'insertion d'une mention dans les contrats, un message d'attente adapté, des affichettes lorsqu'il s'agit par exemple des appels d'urgence depuis les ascenseurs, ou tout autre moyen laissé à l'initiative des entreprises en fonction de leur activité.

C. Les contrôles d'accès à la Banque de France

Afin de sécuriser ses locaux, eu égard au risque important de cambriolage, la Banque de France a souhaité expérimenter des systèmes de contrôle des accès qui mettent en œuvre des procédés techniques originaux. En effet, la CNIL a délivré des avis favorables à deux demandes d'avis, l'une concernant la gestion des accès des salariés à ses comptoirs par la reconnaissance des empreintes digitales et l'autre, la gestion des accès des convoyeurs de fonds par des bornes d'authentification vidéo ; c'est la première fois depuis l'adoption de la loi du n° 95-73 du 21 janvier 1995, que la Commission se trouve saisie d'un système de vidéosurveillance faisant appel à un traitement automatisé d'informations personnelles.

Le contrôle par empreintes digitales s'adresse aux personnes se rendant dans des zones hautement sécurisées c'est-à-dire dans les zones où des fonds

sont stockés ; il repose sur un procédé technique appelé *fingerscan* qui associe un numéro d'identification au contrôle de l'empreinte digitale. La comparaison de l'empreinte du doigt présenté avec l'image numérisée et en trois dimensions d'empreintes des personnes normalement habilitées, préalablement stockées dans une base de données constitue l'application. À terme, une carte à puce sur laquelle seraient enregistrées les caractéristiques de l'empreinte devrait se substituer au numéro. Enfin, outre des numéros d'identification et des empreintes, le dispositif peut enregistrer les heures de passage de 1000 personnes. Le code d'identification et les caractéristiques de l'empreinte stockées dans le fichier sont conservés jusqu'au départ du salarié de la Banque de France, les données liées aux passages n'étant conservées que pendant une durée de trois mois. Les destinataires de ces informations sont les agents de surveillance et la direction.

L'identification des convoyeurs de fonds par des bornes vidéo répond aux risques particuliers encourus par ces personnels. Armés, ces agents sont soumis à une vérification d'identité par les agents de surveillance de la Banque de France, sur la base d'accréditations fournies par les sociétés de transports de fonds qui les emploient. L'identification par la vidéo vient renforcer cette procédure de reconnaissance des personnes, dans la mesure où le gardien effectue un contrôle croisé de la photo numérisée conservée dans une base de données, de l'image de la carte professionnelle placée devant un capteur et des accréditations dûment recensées. Au final, s'affichent sur l'écran du gardien : la photographie préalablement numérisée et enregistrée du convoyeur, l'image de son badge portant sa photographie et l'image en temps réel du convoyeur. Si ces éléments concordent, le gardien procède à l'ouverture.

Le dispositif enregistre le nom de la société de transport de fonds, les nom et prénom du convoyeur, sa photographie, le nom de l'employeur, et enfin, les heures de passage. A terme, le badge du convoyeur comportera également un code barre qui appellera automatiquement la photographie du convoyeur dans le fichier à la disposition du gardien. Les données relatives aux convoyeurs sont conservées tant que ceux-ci sont accrédités par leur société, les informations relatives aux heures de passage sont conservées pendant trois mois.

Délibération n° 97-044 du 10 juin 1997 portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des agents par empreintes digitales

(Demande d'avis n° : 495 531)

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 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le projet d'arrêté présenté par la Banque de France ;

Après avoir entendu Monsieur Hubert Bouchet, en son rapport et Madame Cnarlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ; Considérant que la Banque de France a déposé un demande d'avis relative à la gestion des contrôles d'accès des agents par biométrie des zones sécurisées vers les zones hautement sécurisées des comptoirs de la Banque de France ;

Considérant que le traitement est mis en œuvre dans des sas à unicité de passage ; qu'il utilise la technologie biométrique pour numériser l'empreinte d'un doigt d'une personne ; que les informations enregistrées sont un code d'identification personnel et l'empreinte de la personne ;

Considérant que l'empreinte est numérisée à partir d'un scanner ; que sont pris en comptes notamment l'aspect des tissus, les rides, les plis, le flux sanguins ; que les empreintes de deux doigts sont enregistrées afin d'éviter les rejets en cas de blessures sur le doigt de référence ; Considérant que le dispositif technique ne permet pas de procéder à l'impression des empreintes enregistrées ;

Considérant que le dispositif assure la vérification de la conformité entre l'empreinte préalablement enregistrée et appelée à l'aide d'un code personnel et l'empreinte de la personne qui se trouve dans le sas ; que le système ne permet pas d'identifier un individu ;

Considérant que ce dispositif n'a d'autre finalité qu'assurer la sécurité des zones sensibles ;

Considérant que les salariés concernés seront informés individuellement de l'existence d'un droit d'accès et de rectification ;

Considérant que les informations liées à l'identification de la personne sont conservées jusqu'à son départ du comptoir de la Banque de France ; que les informations liées aux passages des personnes ne seront conservées que pendant une durée de trois mois maximum ;

Considérant que les destinataires de ces informations sont les personnes responsables de la sécurité du comptoir ;

Émet un avis favorable au projet d'arrêté présenté par la Banque de France.

Délibération n° 97-045 du 10 juin 1997 portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des convoyeurs de fonds à l'aide de bornes d'authentifi-cation vidéo

(Demande d'avis n° 495 537)

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 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le projet d'arrêté présenté par la Banque de France ;

Après avoir entendu Monsieur Hubert Bouchet en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ; Considérant que la Banque de France a déposé une demande d'avis relative à la gestion des accès des convoyeurs de fonds par borne d'authentification vidéo ;

Considérant que les convoyeurs de fonds, qui viennent opérer des dépôts ou de retraits importants pour le compte de banques, encourent des risques particuliers et sont armés ; qu'ils sont soumis à une vérification d'identité par les agents de surveillance de la Banque de France, sur la base d'accréditations fournies par les sociétés de transports de fonds qui les emploient ;

Considérant que lorsqu'un camion de convoyage de fonds se présente au comptoir, le gardien qui a à sa disposition une série d'écrans de contrôle, identifie sommairement le camion et le laisse entrer dans le sas qui ne peut contenir qu'un seul véhicule ; que les convoyeurs se présentent les uns après les autres devant la borne d'identification ;

Considérant que la borne dispose d'une caméra qui renvoie l'image du convoyeur et d'une autre qui renvoie l'image de la carte professionnelle placé devant un capteur ; que le gardien recherche alors, à partir du nom de la compagnie de convoyage, le nom du convoyeur qui a fait l'objet d'une accréditation par sa compagnie ;

Considérant que la photographie préalablement numérisée et enregistrée du convoyeur, l'image de son badge portant sa photographie et l'image en temps réel s'affichent sur l'écran du gardien ; que si ces éléments concordent le gardien accorde l'ouverture ;

Considérant que les informations enregistrées sont les nom et prénom du convoyeur, le nom de la société qui l'emploie, les heures de passage des convoyeurs ;

Considérant que les données relatives aux convoyeurs sont conservées tant que le convoyeur est accrédité par sa compagnie ; que les informations relatives aux heures de passage sont conservées pendant trois mois ;

Considérant qu'il appartient à la Banque de France de solliciter régulièrement les compagnies de convoyage de fonds afin qu'elles signalent, avec toute la diligence requise, les personnes qui ne font plus parties des effectifs de l'entreprise, de sorte que le fichier soit constamment à jour ; Considérant que la Banque de France va demander aux sociétés de convoyage d'informer les convoyeurs de la mise en oeuvre de ce système et de l'existence de leur droit d'accès et de rectification ;

Considérant que dans la mesure où la Banque de France n'entretient pas de relations directes avec les convoyeurs de fonds, ce mode d'information est satisfaisant ;

Émet un avis favorable au projet d'arrêté présenté par la Banque de France.

III. L'EVALUATION DES RISQUES PROFESSIONNELS

A. Les fonctions publiques et hospitalières

La Caisse des dépôts et consignations a saisi la Commission d'une demande d'avis relative à un modèle type de traitement automatisé d'informations nominatives destiné à recueillir des données sur les risques professionnels auxquels sont exposés les agents des fonctions publiques et hospitalières. Cette application baptisée « PRORISQ » doit assurer la gestion de ces risques par métier, faciliter les indemnisations en cas d'accidents du travail ou de maladies professionnelles, produire des statistiques afin de prévoir des politiques nationale et locales de prévention.

En pratique, « PRORISQ » utilise des données transmises aux employeurs : il s'agit des nom et prénom, du numéro de sécurité sociale conformément au décret n° 85-420 du 3 avril 1985, des circonstances de l'accident et de l'activité (horaires de travail et déroulement de carrière) ; seuls les médecins du travail sont destinataires de données médicales. Il est prévu que les ministères des Affaires sociales, de l'Intérieur, de la Fonction publique, la CNAMTS et divers organismes de recherche (CNRS, INSERM...) reçoivent des informations statistiques sous forme de tableaux de données agrégées, le seuil minimal étant départemental.

Dans la mesure où il s'agit d'informations couvertes par le secret médical et le secret professionnel, la CNIL a relevé avec satisfaction que les mesures de sécurité étaient intégrées à l'application informatique, de sorte qu'aucun employeur ne puisse diminuer le niveau de protection des données ; les 3 500 employeurs potentiellement intéressés par « PRORISQ », devront, préalablement, à l'implantation du système, déposer une déclaration simplifiée en référence à ce modèle auprès de la CNIL.

Délibération n° 97-037 du 27 mai 1997 portant avis sur un modèle type présenté par la Caisse des dépôts et consignations dénommé « PRORISQ » et ayant pour finalité le recueil des données concernant les risques professionnels dans les fonctions publiques territoriale et hospitalière

(Demande d'avis n° 485 469)

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 pris pour l'application de la loi du 6 janvier 1978 susvisée ;

Vu le décret n° 47-1846 du 19 septembre 1947 modifié portant règlement d'administration publique pour la constitution de la caisse nationale de retraite prévue à l'article 3 de l'ordonnance n° 45-993 du 17 mai 1945 relative aux services publics des départements et des communes et leurs établissements publics ;

Vu le décret n° 85-420 du 3 avril 1985 relatif à l'utilisation du répertoire national d'identification des personnes physiques par des organismes de sécurité sociale et de prévoyance ;

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

Considérant que la Caisse des dépôts et consignations a déposé auprès de la Commission un dossier de demande d'avis ayant pour objet la mise en œuvre d'un modèle type de traitement automatisé d'informations nominatives, qui sera mis à la disposition des employeurs des agents régis par les fonctions publiques territoriale et hospitalière ;

Considérant que ce traitement a pour finalité principale d'assurer la gestion des risques professionnels par métiers, de faciliter les indemnisations des agents victimes d'accident du travail ou de maladie professionnelle ; qu'il sert également à produire des statistiques non nominatives à l'attention de différents organismes publics, à définir les risques professionnels par métier, ainsi qu'à prévoir une politique nationale en matière de prévention des risques ;

Considérant que le traitement « PRORISQ » permet à chaque employeur de générer ses propres statistiques afin de définir sa propre politique de prévention ;

Considérant que lorsqu'un agent est victime d'un accident du travail, l'employeur constitue un dossier de demande d'indemnisation qui est envoyé à la commission de réforme départementale, laquelle délivre un avis transmis à la caisse nationale de retraite des agents des collectivités locales qui procède à l'étude du droit de la personne à l'aide d'un dossier complet comportant également les pièces médicales ;

Considérant que l'avis rendu par la CNRACL lie la collectivité ; qu'il est transmis à l'employeur et à l'agent concerné ;

Considérant qu'il est prévu, à terme, une dématérialisation des circuits de transmission des informations à l'exception, toutefois, des données médicales ;

Considérant qu'il appartient à l'agent de fournir un certificat médical, à l'appui de sa demande d'indemnisation d'accident du travail, et au médecin du travail de transmettre l'information directement à la commission de réforme lorsqu'il s'agit d'une maladie professionnelle ;

Considérant que les données nominatives enregistrées sont le nom patronymique, le nom marital, le prénom, la date de naissance, le numéro de sécurité sociale, le numéro d'affiliation à la CNRACL, l'activité exercée, les horaires de travail, l'expérience professionnelle, les circonstances et le coût de l'accident du travail, accident de trajet ou accident survenu en cours de mission, les lésions et leur siège sous une forme codée, les maladies professionnelles et le coût médical de l'accident ; que ces données paraissent pertinentes au regard de la finalité poursuivie ;

Considérant que ces informations sont conservées jusqu'au décès de la personne ou jusqu'à la date de rétablissement de l'actif au régime général ;

Considérant que les destinataires d'informations nominatives sont les services des ressources humaines des employeurs chargés de la gestion des déclarations d'accidents et de maladies professionnelles ; que les médecins du travail sont seuls destinataires des données médicales autres que les codifications retenues ;

Considérant que les agents de la Caisse des dépôts et consignations sont destinataires d'informations permettant l'ouverture et la détermination des droits des agents (numéro CNRACL, vie professionnelle, déplacements des personnes et santé) ; que les assureurs intervenant dans le cadre de contrats de réassurance du risque accident du travail des agents avec les employeurs sont destinataires des nom et prénom de l'agent concerné, du code de la lésion, la vie professionnelle et, s'il s'agit d'un accident de trajet ou d'un accident survenu en cours de mission ;

Considérant, que des statistiques anonymes sont fournies sous forme de tableaux aux ministères des Affaires sociales, de l'Intérieur, de la Fonction publique, au CNRS, à l'INSERM, à l'INRS, à l'ATIACL, aux centres de recherche universitaires ou publics, à Eurostat et à la CNAMTS ;

Considérant que les mentions de l'article 27 de la loi seront apposées sur les formulaires de déclarations d'accidents ou de maladies professionnelles que remplissent les personnes concernées ;

Considérant que les mesures de sécurité mises en œuvre par la CDC pour garantir la confidentialité et l'intégrité des données apparaissent satisfaisantes ; qu'il est prévu la mise en place de mots de passe de huit caractères modifiés tous les trois mois, ainsi que trois niveaux différents d'habilitation ;

Considérant que lorsque « PRORISQ » sera installé chez un employeur, les mesures de sécurité seront alors initialisées et figées ; que, par ailleurs, ces informations sont couvertes par le secret médical ainsi que par le secret professionnel ;

Considérant que les employeurs utilisant ce traitement devront faire une déclaration simplifiée en référence au présent modèle type accompagnée d'une annexe décrivant les sécurités, notamment physiques, mises en œuvre ;

Émet un avis favorable au projet d'acte réglementaire présenté par la Caisse des dépôts et consignations.

B. Le transport routier

La conduite et l'exploitation de véhicules de transport routier de voyageurs et de marchandises, publics comme privés, sont soumises à des obligations relatives à la durée du travail, notamment la répartition des périodes d'activité et de repos. Le respect de ces obligations, définies par le règlement européen n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route, est vérifié grâce à un appareil spécifique placé à bord des véhicules. Cet appareil de contrôle, appelé « chronotachygraphe », permet l'édition, sur une feuille de route, des périodes de conduite, de travail et de disponibilité.

La CNIL a émis un avis favorable à la mise en œuvre d'un traitement national destiné à contrôler les conditions de travail des conducteurs de véhicules de transports routiers. Ce traitement, dénommé « SCAN RÉSO » et présenté à l'initiative du ministre de l'Équipement, des Transports et du Logement, doit faciliter la détection d'éventuelles infractions à la législation sociale en déchiffrant, par un procédé de lecture optique, les relevés effectués par les appareils de contrôle embarqués à bord de ces véhicules.

À cet effet, sont enregistrées dans le traitement « SCAN RÉSO » : l'identité du représentant légal de l'entreprise, dont la responsabilité peut être engagée au titre pénal et celle du conducteur dont les disques ont été relevés ; de plus, le traitement prévoit la collecte de l'immatriculation et du kilométrage parcouru du véhicule, les temps mémorisés par le chronotachygraphe, ainsi que, le cas échéant, le nombre d'infractions relevées.

La durée de conservation des informations traitées varie selon que des infractions ont été ou non constatées et selon que les procès-verbaux correspondants ont ou non été transmis au parquet compétent.

Si aucun procès-verbal n'est adressé au procureur de la République, l'ensemble des informations nominatives traitées est détruit dès l'envoi au responsable légal de l'entreprise concernée du courrier de notification de la clôture de l'instruction du contrôle.

En cas de transmission au parquet, seules les informations concernant les conducteurs ayant commis des infractions sont visées ; ces informations sont en principe conservées durant le délai de prescription de l'action publique, soit trois années après la transmission au parquet pour les délits et un an pour les contraventions, lorsqu'aucune suite connue n'a été donnée par le parquet.

Ce principe souffre toutefois des exceptions : ainsi, les informations sont-elles effacées dès réception d'un avis de classement sans suite ou de la notification d'un jugement définitif non frappé d'appel. À l'inverse, les informations sont conservées au-delà du délai de prescription de l'action publique lorsque des poursuites (qui interrompent ce délai) sont engagées : dans ce cas, les informations sont effacées dès réception du jugement ou de l'appel définitif.

Délibération n° 97-096 du 16 décembre 1997 relative à la demande d'avis présentée par le ministère de l'Équipement, des Transports et du Logement portant création d'un traitement automatisé ayant pour finalité le contrôle des conditions de travail des conducteurs routiers « SCAN RÉSO »

(Demande d'avis n° 518 712)

La Commission nationale de l'informatique et des libertés ;

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

Vu le règlement (CEE) n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route ;

Vu le règlement (CEE) n° 3821/85 du Conseil du 20 décembre 1985 modifié concernant l'appareil de contrôle dans le domaine des transports par route ;

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

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

Vu le décret n° 86-1130 du 17 octobre 1986 modifié relatif à l'application des dispositions du règlement (CEE) n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route et du règlement (CEE) n° 3821/85 du Conseil du 20 décembre 1985 modifié concernant l'appareil de contrôle dans le domaine des transports par route ;

Vu l'ordonnance n° 58-1310 du 23 décembre 1958 modifiée concernant les conditions de travail dans les transports routiers publics ou privés en vue d'assurer la sécurité de la circulation routière ;

Vu le projet d'arrêté du ministre de l'Équipement, des Transports et du Logement ;

Après avoir entendu Madame Isabelle Jaulin, 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 a été saisie par le ministre de l'Équipement, des Transports et du Logement d'un projet d'arrêté portant création d'un traitement national dénommé « SCAN RÉSO » appelé à être mis en oeuvre dans l'ensemble des directions régionales et départementales de l'équipement et relatif au contrôle des conditions de travail des conducteurs de véhicules de transports routiers ;

Considérant que ce traitement a pour finalité la lecture optique des diagrammes inscrits sur les feuilles d'enregistrement (disques) des appareils de contrôle installés à bord des véhicules de transport routier, l'exploitation des données enregistrées sur ces disques afin de calculer les temps de conduite, de travail, de disponibilité et de repos des conducteurs de ces véhicules, la recherche d'éventuelles infractions et la fourniture, le cas échéant, des éléments permettant d'établir des procès-verbaux ;

Considérant que l'ordonnance du 23 décembre 1958 concernant les conditions de travail dans les transports routiers publics et privés en vue d'assurer la sécurité de la circulation routière prévoit notamment dans son article premier que la conduite et l'exploitation de véhicules de transport routier de voyageurs et de marchandises, publics comme privés, sont soumis à un certain nombre d'obligations relatives à la durée du travail, notamment la répartition des périodes de travail et de repos ;

Considérant que ces obligations sont définies par l'article 6 du règlement européen n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route ; que le règlement n° 3821/85 du Conseil du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des

transports par route a imposé l'installation dans les véhicules de transports de passager ou de marchandises d'un appareil de contrôle — dit « chrono-tachygraphe » — qui procède automatiquement sur une feuille de route au relevé des périodes de conduite, des autres périodes de travail, ainsi que des périodes de disponibilité des chauffeurs ;

Considérant que l'article 2 de l'ordonnance précitée met notamment à la charge des inspecteurs et des fonctionnaires ou agents de l'État chargés du contrôle des transports terrestres sous l'autorité du ministre chargé des Transports de constater les infractions aux dispositions législatives ou réglementaires concernant les obligations visées à son article premier ; qu'aux termes de ce texte, ces agents ont accès à l'appareil de contrôle et à toutes ses composantes afin d'en vérifier l'intégrité et que leurs procès-verbaux font foi jusqu'à preuve contraire ;

Considérant que les informations enregistrées sont, s'agissant du représentant légal de l'entreprise et, le cas échéant, de l'interlocuteur lors de la visite, leur nom, prénom, titre, qualité, ainsi que l'adresse de l'entreprise ; que s'agissant des conducteurs, sont enregistrés leur nom, prénom, qualité, ainsi que le nombre de disques prélevés et le nombre de disques lus et, pour chaque disque prélevé, l'immatriculation et le kilométrage parcouru par le véhicule, les temps enregistrés par le chronotachygraphe, ainsi que, le cas échéant, le nombre d'infractions relevées ;

Considérant que ces informations sont pertinentes au regard de la finalité du traitement ;

Considérant que la durée de conservation des informations traitées varie selon que le contrôle donne lieu ou non à transmission d'un procès-verbal au parquet ; qu'en l'absence de saisine du parquet, l'ensemble des informations traitées sont détruites dès l'envoi au responsable légal de l'entreprise concernée du courrier de notification de la clôture de l'instruction du contrôle ; qu'en cas de saisine du parquet, les informations traitées sont conservées, sauf réception d'un avis de classement sans suite, durant le délai de prescription de l'action publique, soit trois années après cette transmission pour les délits ou une année pour les contraventions, ou jusqu'à la date de réception de la décision judiciaire devenue définitive ; que les informations traitées sont effacées au-delà de cette date ;

Considérant que cette durée de conservation est pertinente au regard de la finalité du traitement ;

Considérant que les destinataires des informations traitées sont, chacun pour ce qui le concerne et dans la limite de leurs attributions, les préfets de région et de département, le directeur des transports terrestres, les directeurs régionaux et départementaux de l'équipement, les membres des corps d'inspection, les parquets quand une infraction fait l'objet d'un procès-verbal, ainsi que le représentant légal de l'entreprise ;

Considérant que le droit d'accès s'exerce auprès du service des transports de la direction régionale de l'équipement ou de la cellule transport départementale de l'équipement concernée, résidence administrative du contrôleur des transports qui a effectué le contrôle ;

Considérant que les intéressés en sont informés par un courrier, adressé au responsable légal de l'entreprise, qui précise également les catégories d'informations traitées pour chaque catégorie de personnel, ainsi que leur durée de conservation ; que ce courrier invite en outre le responsable de

l'entreprise à informer les intéressés de leurs droits au regard des dispositions de la loi du 6 janvier 1978 ;

Considérant qu'en application du second alinéa de l'article 26 de la loi du 6 janvier 1978, le projet d'acte réglementaire exclut la possibilité pour les intéressés de se prévaloir, à l'égard de ce traitement, de la faculté d'opposition énoncée par l'alinéa premier de cet article ;

Émet un avis favorable au projet d'arrêté du ministre de l'Équipement, des Transports et du Logement portant création d'un traitement national dénommé « SCAN RÉSO »

IV. LA DECLARATION UNIQUE À L'EMBAUCHE

Le système de déclaration unique à l'embauche a été institué par le décret n° 95-1355 du 29 décembre 1995, afin de simplifier les démarches administratives que se doit d'accomplir un employeur. En effet, la déclaration unique d'embauche (DUE) rassemble les onze formalités qui peuvent s'imposer préalablement à une embauche, sur un seul support qui est alors adressé par courrier, minitel ou fax à l'URSSAF, interlocuteur unique qui se chargera de les ventiler sur les différents partenaires habilités à en connaître.

La CNIL s'est prononcée favorablement sur la demande d'expérimentation du traitement lié à l'institution de la déclaration unique d'embauche présenté par l'agence centrale des organismes de sécurité sociale (ACOSS). Toutefois, à cette occasion, la CNIL avait souligné que le numéro d'inscription au répertoire (NIR) des salariés, légalement collecté au titre de la déclaration préalable à l'embauche, ne devait être transmis qu'aux seuls organismes habilités. Par ailleurs, la Commission avait demandé que des mesures soient prises pour garantir l'intégrité des données envoyées par l'employeur (cf. 17^{e} rapport, p. 356).

En 1997, la CNIL a été saisie de la généralisation de ce dispositif, assortie de quelques modifications qui prennent en compte d'une part, les évolutions législatives et réglementaires, notamment en matière de demandes d'exonérations ou des aides à l'emploi, d'autre part, les changements techniques et fonctionnels induits par la mise en place définitive du traitement.

À cette occasion, la Commission a délivré un avis favorable en saluant les améliorations apportées au système. En effet, la CNIL a tout d'abord relevé le renforcement des procédures de contrôle de vraisemblance et de cohérence visant à assurer la qualité des informations transmises aux partenaires, et les efforts réalisés concernant la lisibilité du formulaire unique. De même, pour répondre à son souci relatif au manque de fiabilité des données transmises, il est désormais prévu que les employeurs puissent suivre par minitel les étapes des formalités accomplies ; ainsi, l'employeur peut obtenir à partir du numéro de SIRET, la liste des salariés ayant fait l'objet d'une DUE, et l'application propose l'accès au dossier de formalités sur lequel un employeur souhaite

intervenir en modification, en annulation ou en complément. Par ailleurs, d'importantes améliorations techniques ont permis de fiabiliser la gestion du code d'accès minitel par l'employeur. Enfin, au plan de l'architecture, les serveurs de DUE vont être implantés dans l'environnement sécurisé des centres régionaux de traitement informatique du recouvrement, qui hébergent les bases de données des DUE individualisées pour chaque URSSAF.

Délibération n° 97-001 du 14 janvier 1997 portant avis sur le projet d'acte réglementaire présenté par l'ACOSS concernant la modification du traitement relatif à la gestion de la déclaration unique à l'embauche

(Demande d'avis n° 409 224)

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 code du travail et notamment ses articles L. 320, L. 311-5, R. 241-48, R. 320-1 et R. 351-2 ;

Vu le code de la sécurité sociale et notamment ses articles L. 312-1 et R. 243-14 ;

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° 95-1355 du 29 décembre 1995 instituant une déclaration unique à l'embauche ;

Vu la délibération n° 93-055 de la CNIL du 29 juin 1993 portant avis favorable sur le traitement relatif à la gestion de la déclaration préalable à l'embauche ;

Vu la délibération n° 96-005 de la CNIL du 20 février 1996 portant avis favorable sur une demande présentée par l'agence centrale des organismes de sécurité sociale (ACOSS) relative à la mise en oeuvre, par les URSSAF, d'un traitement automatisé d'informations nominatives ayant pour finalité la gestion de la déclaration unique à l'embauche « DUE » ;

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

Considérant que l'agence centrale des organismes de sécurité sociale (ACOSS) a saisi la Commission d'une demande d'avis portant modification du traitement relatif à la gestion de la déclaration unique d'embauche ; que cette modification constitue la généralisation de l'expérimentation menée pendant l'année 1996 ;

Considérant que cette modification a pour objet de prendre en compte les évolutions législatives et réglementaires ainsi que les modifications techniques et fonctionnelles induites par la mise en place définitive du dispositif ;

Considérant ainsi que certaines mesures d'exonération et d'aide à l'emploi telles que les exonérations des cotisations patronales au titre des deuxièmes

et troisièmes embauches et l'aide au premier emploi des jeunes (APEJ) sont devenues caduques ; qu'en revanche la conclusion de conventions de contrat initiative emploi ouvrant droit à une aide spécifique et la demande d'exonération des cotisations patronales pour l'embauche du quatrième au cinquantième salarié institué par l'article 58 de la loi n° 95-116 du 4 février 1995 ont été intégrées dans le dispositif ;

Considérant que les modifications apportées consistent également à améliorer la qualité des informations transmises aux partenaires par un renforcement des procédures de contrôle de vraisemblance et de cohérence et par une présentation plus claire de la déclaration ;

Considérant que conformément à la demande exprimée par la Commission dans sa délibération du 20 février 1996 qui souhaitait que « des mesures particulières soient prises dans le souci de lever toute incertitude de la part de l'employeur sur l'intégrité des données finalement réceptionnées par l'organisme destinataire et sur le caractère régulier et complet de la déclaration qu'il a accomplie », une modification du dispositif a été réalisée ; qu'ainsi, l'employeur peut désormais suivre par minitel les étapes de ses formalités administratives d'embauche ;

Considérant que les traitements seront mis en œuvre sur des serveurs désormais implantés dans les centres régionaux de traitement informatique du recouvrement (CERTI) disposant de mesures de sécurité appropriées ;

Considérant que les durées de conservation des données prévues par les conventions conclues avec la CNAMTS, la CNAVTS, le ministère du Travail et l'UNEDIC sont de deux ans et neuf mois à compter de la date de réception des informations par l'URSSAF ; que pendant cette durée les partenaires peuvent demander à l'organisme de recouvrement copie des éléments déclaratifs les concernant ;

Émet un avis favorable au projet d'acte réglementaire présenté par l'ACOSS.

Demande à être saisie de toute modification ultérieure du dispositif.

Chapitre 11

TELECOMMUNICATIONS

I. LA LISTE UNIVERSELLE DES ABONNES AU TÉLÉPHONE

Dans le cadre des dispositions prévues par la loi n° 96-659 du 26 juillet 1996 réglementant les télécommunications, le ministère délégué à la Poste, aux Télécommunications et à l'Espace a saisi la CNIL d'un projet de décret en Conseil d'État relatif aux modalités de mise en œuvre de l'annuaire dit « universel », appelé à se substituer, à partir du 1er janvier 1998, à l'annuaire des abonnés au réseau de téléphonie fixe de France Télécom. En effet, dans le contexte de la déréglementation du secteur des télécommunications, un organisme juridique distinct des opérateurs est chargé d'établir une liste dite universelle regroupant les coordonnées de l'ensemble des personnes abonnées au téléphone, quel que soit l'opérateur concerné.

À la lumière de ces textes, la CNIL a d'abord constaté avec satisfaction que les droits actuellement reconnus aux abonnés étaient consacrés, notamment le droit de s'opposer :

— à ce que leurs coordonnées figurent dans un annuaire téléphonique ou soient divulguées par un service de renseignements téléphoniques accessibles au public (inscription en liste rouge) ;

— à l'utilisation de leurs coordonnées à des fins, notamment commerciales, autres que l'édition d'annuaires (inscription en liste orange) ;

— à ce que figure dans l'annuaire leur prénom, ou toute information susceptible de révéler leur sexe.

La Commission a également noté avec satisfaction que l'abonné a désormais le droit de ne pas faire figurer dans l'annuaire son adresse complète, dans la mesure où cela ne génère pas de risque d'homonymie.

Sur la base de ces dispositions légales, la liste universelle fournie pour l'édition d'annuaires ou la fourniture de services de renseignements téléphonique doit être expurgée des données concernant les personnes inscrites en liste rouge, tandis que pour toute autre utilisation, notamment commerciale, elle sera expurgée des données concernant les personnes inscrites en liste rouge et en liste orange.

À cette occasion, la CNIL a également examiné les risques liés à la perspective d'une diffusion des services de l'annuaire sur Internet ou sur CD ROM. Ainsi, et alors même que cela ne faisait l'objet d'aucune disposition particulière dans le projet de décret, la Commission a indiqué les garanties spécifiques qui devraient être offertes aux personnes dans une telle hypothèse. La CNIL a en effet estimé qu'il convenait d'offrir aux abonnés la faculté de s'opposer gratuitement à la diffusion sur Internet d'informations les concernant, en particulier pour limiter l'accès depuis le territoire d'un État n'assurant pas aux données personnelles une protection équivalente à celle garantie par la loi française.

Par ailleurs, le projet de décret prévoyait la possibilité pour certains services de l'État de consulter de façon permanente la liste universelle, dont il convient de rappeler qu'elle comprend la liste rouge (environ 5,6 millions abonnés). La Commission a estimé que les services d'urgence et de sauvegarde de la vie humaine (SAMU, pompiers, police-secours) étaient fondés à accéder aux données issues de la liste universelle nécessaires pour l'exercice de leurs missions. Il convient de rappeler à cet égard que la Commission s'était déjà prononcée favorablement au sujet de la présentation systématique de tous les numéros appelant, y compris ceux de la liste rouge, pour le 18 : pompiers, le 15 : SAMU, et le 17 : police secours (cf. 13^{e} rapport, p. 226, 14^{e} rapport, p. 317, 15^{e} rapport, p. 373, 17^{e} rapport, p. 362).

En revanche, la Commission a suggéré que l'ouverture de l'accès à la liste rouge soit davantage encadrée en ce qui concerne la possibilité d'une consultation électronique permanente de la liste rouge par les services de l'État en application des dispositions relatives aux interceptions de sécurité (article 22 de la loi 91-646 du 10 juillet 1991), aux enquêtes de flagrance et aux enquêtes préliminaires (respectivement articles 53 et *75* du code de procédure pénale). En effet, la consultation de la liste rouge par les services de l'État était, jusqu'alors, réservée uniquement aux services de police judiciaire agissant sur commission rogatoire d'un juge d'instruction ou dans le cadre d'une enquête de flagrance, les enquêtes préliminaires étant légalement dépourvues de tout effet coercitif, sauf consentement exprès, c'est-à-dire écrit, de la personne concernée. Dès lors, la CNIL a relevé que le mode de consultation envisagé par le projet de décret ne permettait pas de distinguer les cadres juridiques dans lesquels les consultations de la liste rouge seraient effectuées et a exprimé une réserve sur ce point. À ce jour, ce décret n'a toujours pas été publié.

Délibération n° 97-010 du 4 février 1997 portant avis sur le projet de décret d'application de l'article L. 35-4 du code des postes et télécommunications relatif à l'annuaire universel

La Commission nationale de l'informatique et des libertés,

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

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

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

Vu le code de procédure pénale ;

Vu la loi n° 91-646 du 10 juillet 1991relative au secret des correspondances émises par la voie des télécommunications ;

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation de télécommunications ;

Vu le projet de décret d'application de l'article L. 35-4 du code des postes et télécommunications ;

Considérant que la loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications a confié à un organisme juridiquement distinct des entreprises offrant des biens et des services de télécommunications le soin d'établir et de tenir à jour la liste nécessaire à l'édition d'un annuaire universel regroupant, sous forme d'un document papier ou électronique, les coordonnées de l'ensemble des abonnés à un réseau téléphonique ;

Considérant que l'article L. 35-4, introduit par cette loi dans le code des postes et télécommunications, renvoie à un décret en Conseil d'État, pris après avis de la Commission supérieure du service des postes et télécommunications, le soin de préciser « les missions confiées à cet organisme et les garanties à mettre en oeuvre pour assurer la confidentialité des données, notamment au regard des intérêts commerciaux des opérateurs, et la protection de la vie privée » ;

Considérant que le ministre délégué à la Poste, aux Télécommunications et à l'Espace a saisi la CNIL, le 17 décembre 1996, de ce projet de décret qui apporte des précisions tant sur les modalités de tenue et de mise à jour de la liste universelle que sur les dispositions relatives aux droits des abonnés ;

Considérant que ce projet prévoit que l'organisme, dont le mode de désignation est fixé par l'article R. 20-44-1nouveau, sera chargé d'établir et de tenir à jour la liste de tous les abonnés connectés aux réseaux ou services téléphoniques, dénommée « liste universelle », qui contient les informations nominatives suivantes : nom, prénom, adresse et numéro de téléphone ainsi que la mention de la profession pour les abonnés qui le souhaitent ;

Considérant que ces informations seront transmises, chacun pour ce qui le concerne, par chaque opérateur qui les aura préalablement recueillies auprès de ses propres abonnés ;

Considérant que les opérateurs devront également communiquer à l'organisme les informations relatives aux abonnés inscrits en liste rouge ou en liste orange selon les modalités précisées par l'article R. 20-44-3 nouveau ;

Considérant que l'article R. 20-44-6 nouveau précise que la production et le contenu des bases de données qui seront transmises à l'organisme relèvent de la responsabilité des opérateurs ou de leurs distributeurs, sous réserve de la responsabilité propre de l'organisme dans la conduite des tâches qu'il accomplit, cet organisme étant tenu, par les dispositions de l'article R. 20-44-8, de prendre les mesures nécessaires pour préserver la sécurité physique et logique des données qu'il détient ;

S'agissant des droits reconnus aux abonnés

Considérant que l'article R. 10-1nouveau prévoit le droit pour tout abonné de s'opposer à la divulgation des informations nominatives le concernant (liste rouge), de s'opposer à l'utilisation de ces informations dans les opérations commerciales (liste orange) et de s'opposer à ce que figure dans l'annuaire son adresse complète ainsi que son prénom ou toute information susceptible de révéler son sexe dans la mesure où l'exercice de ce droit ne générerait pas de risque d'homonymie ;

Considérant que le droit à ce que ne figure pas dans un annuaire l'adresse complète de l'abonné constitue une garantie efficace pour préserver la vie privée de même que le droit de ne pas faire figurer son prénom ou toute information susceptible de révéler son sexe ; qu'il y a lieu toutefois sur ce dernier point de relever que la plupart des prénoms révèle en France l'identité sexuelle ;

Considérant qu'il y aurait lieu que le décret précise si l'absence de risque d'homonymie doit être appréciée par l'opérateur auprès duquel la personne concernée est abonnée — auquel cas le risque ne pourra être décelé qu'au regard d'une liste partielle des abonnés — ou par l'organisme auquel est confiée la tenue de la liste universelle ; que l'article R. 20-44-7 nouveau devra retenir au deuxième tiret du 1, la même rédaction que celle qui figurera à l'article R. 10-1nouveau ;

Considérant que l'article R. 20-44-5 nouveau précise les conditions de diffusion par l'organisme de la liste universelle et des listes qui en seront extraites ; que la diffusion de ces listes fera l'objet de licences d'utilisations délivrées par l'organisme aux différentes catégories d'utilisateurs, les conditions générales de ces licences, devant être publiées après avis du ministre chargé des Télécommunications ;

Considérant que les conditions de diffusion seront différentes selon l'usage des données projeté afin d'assurer la protection des droits des abonnés ; qu'il est ainsi fait une distinction entre la diffusion d'informations aux fins d'édition d'annuaires ou de fournitures de services de renseignements, cas dans lequel l'organisme mettra à la disposition du demandeur la « liste universelle » ou des extraits de celle-ci, expurgée des seules données concernant les personnes inscrites en liste rouge, et la diffusion d'informations aux fins de toute autre utilisation, notamment commerciale, auquel cas l'organisme mettra à la disposition de toute personne qui lui en fera la demande des listes préalablement expurgées des données concernant les personnes inscrites en liste rouge et des données concernant les personnes inscrites en liste orange ;

Considérant que ce texte prévoit que cette mise à disposition sera faite moyennant une juste rémunération reflétant les coûts et tenant compte de l'usage projeté des informations ;

Considérant que ce même texte précise que la liste Safran qui regroupe, en application de la loi n° 89-1008 du 31décembre 1989, les personnes ne souhaitant pas faire l'objet d'un démarchage publicitaire par voie de télex ou de télécopie, sera mise à disposition par l'organisme à un prix reflétant alors les coûts de gestion, l'usage projeté des informations n'étant pas pris en compte dans le coût de diffusion ;

Considérant que le sixième alinéa de l'article R. 10-1nouveau interdit l'usage par quiconque dans des opérations commerciales des données identifiantes extraites des fichiers d'abonnés et relatives aux abonnés inscrits en liste orange, la contravention à ces dispositions étant punie pour chaque information mise en circulation de l'amende prévue pour les contraventions de troisième classe ;

Considérant qu'il y a lieu de souligner que les nouvelles techniques de l'information et le développement des architectures en réseaux internationaux permettent désormais de constituer non seulement des annuaires sur support papier ou sur un support électronique accessible depuis le seul territoire national mais aussi des annuaires sur un support électronique nomade — tel est le cas des annuaires sur CD-ROM — ou sur un réseau international ouvert ; que ces circonstances doivent amener à s'interroger sur la portée des garanties ainsi offertes par le projet de décret, surtout lorsque les données figurant dans un annuaire qui comportera notamment celles relatives aux personnes s'étant opposées à toute utilisation commerciale des informations les concernant, pourront être accessibles depuis le territoire d'un État n'assurant pas aux données personnelles une protection équivalente à celle garantie par la loi française ;

Considérant que le souci d'une exacte information des personnes sur les risques particuliers que la diffusion d'informations les concernant génère lorsque ces données sont aisément téléchargeables, notamment via Internet, depuis le territoire d'un État n'assurant pas aux données de protection particulière, devrait conduire à prévoir dans ce cas un dispositif particulier ;

Considérant en effet, qu'il convient, d'une part, de relever que l'article 12 de la Convention du 28 janvier 1981du Conseil de l'Europe subordonne les flux transfrontières de données à caractère personnel à l'assurance que la réglementation de l'État de destination des données apporte une protection équivalente à celle offerte par cette Convention ; que la directive récemment adoptée par le Conseil du Parlement européen sur la protection des données personnelles et la libre circulation des données prévoit que les flux transfrontières de données ne peuvent, en principe, avoir lieu qu'en direction d'un État assurant un niveau de protection adéquat ;

Considérant, d'autre part, qu'il convient de rappeler que la CNIL recommande, de manière générale, que lorsque des données nominatives sont diffusées sur Internet, les personnes concernées soient clairement informées des risques inhérents à la nature de ce réseau et de leur droit de s'opposer à une telle diffusion ;

Considérant dès lors qu'il paraît nécessaire que l'article R. 10-1nouveau soit complété, dans son premier alinéa, par une disposition ainsi rédigée : « À ce que ne soit pas mentionnées les données nominatives la concernant dans un annuaire distribué ou diffusé sur un support électronique accessible depuis le territoire d'un État n'assurant pas aux données personnelles une

protection équivalente à celle garantie par la loi française », et que l'exercice de ce droit soit gratuit.

S'agissant de l'accès par des autorités habilitées à la « liste universelle »

Considérant que l'article R. 20-44-9 nouveau prévoit que l'organisme satisfait aux demandes d'informations de certaines autorités habilitées par le biais d'une possibilité permanente de consultation électronique de la « liste universelle » dont les modalités sont déterminées par une convention entre l'organisme et les services de l'État concerné ;

Considérant, en premier lieu, que l'article R. 20-44-9 nouveau ne vise pas la totalité des autorités actuellement habilitées à bénéficier de l'accès aux informations concernées (ainsi, parmi d'autres, le service des impôts en application de l'article L. 83 du livre des procédures fiscales, la Commission des opérations de bourse en application des articles 5Ì et 5B de l'ordonnance n° 67-833 du 28 septembre 1967 ou encore la Banque de France et la Commission bancaire en application de l'article *57* de la loi n° 84-46 du 28 janvier 1984) ; qu'il n'apparaît pas nécessaire de citer les autorités en cause dès lors que la simple mention des « autorités habilitées » suffit, sur le fondement des textes ayant institué leur habilitation, à la compréhension du texte de l'article ;

Considérant, en deuxième lieu, que sont visées, au titre des autorités habilitées bénéficiaires, moyennant une juste rémunération, de ce service, les autorités visées par l'article 22 de la loi du 10 juillet 1991relative au secret des correspondances ainsi que les autorités agissant en application des articles 53 et *75* du code de procédure pénale ; qu'il résulte de la référence faite à l'article 75 du code de procédure pénale relatif à l'enquête préliminaire, que les officiers de police judiciaire et, sous le contrôle de ceux-ci les agents de police judiciaire, procédant, y compris d'office, par voie d'enquête préliminaire, pourraient accéder aux informations portées sur la « liste universelle » concernant des personnes inscrites en liste rouge ;

Considérant qu'à l'heure actuelle et conformément à une instruction de France Télécom n° 94 216 du 26 décembre 1994, le procureur de la République ou son substitut ainsi que tout officier de police judiciaire agissant dans le cadre d'un enquête préliminaire ne peuvent avoir accès aux informations relatives aux personnes inscrites sur liste rouge ; qu'en effet, dans ce cadre juridique, et à la différence des missions de police judiciaire qui peuvent être accomplies dans le cadre de l'instruction préparatoire en application des dispositions des articles 81et suivants du code de procédure pénale et, en application des dispositions des articles 53 et suivants, dans le cadre de l'enquête de flagrance, les officiers de police judiciaire ne peuvent procéder à des perquisitions, visites domiciliaires et saisies sans l'assentiment exprès de la personne chez laquelle ces opérations ont lieu ; que ces dispositions sont généralement interprétées comme ne permettant pas à ces personnels, dans ce cadre juridique, d'avoir accès à des informations juridiquement protégées ; que par suite, à défaut de dispositions législatives particulières, les officiers de police judiciaire, agissant par voie d'enquête préliminaire, ne sauraient se voir conférer la qualité de tiers autorisé, au sens de l'article 29 de la loi du 6 janvier 1978, à avoir accès aux informations figurant sur la liste rouge ; qu'en fout état de cause, il apparaît souhaitable de ne pas étendre dans des proportions qui devien-

draient trop importantes, le champ des dérogations au caractère confidentiel de la liste rouge ;

Considérant, en troisième lieu, que les autorités habilitées en vertu de dispositions particulières à avoir accès à des informations issues d'un traitement automatisé placé sous la responsabilité d'un tiers ne sauraient, sauf à ce que la finalité du traitement le justifie, avoir un accès permanent et portant sur la totalité des informations nominatives enregistrées dans le fichier ; qu'en revanche la qualité de tiers autorisé, au sens de l'article 29 de la loi du 6 janvier 1978, permet à ces autorités habilitées d'avoir un accès ponctuel à des informations nominatives détenues par des tiers ; que tel est notamment le cas, en application de l'article 22 de la loi du 10 juillet 1991, des juridictions et autorités compétentes pour ordonner des interceptions des correspondances émises par la voie des télécommunications, ou encore du procureur de la République et des officiers de police judiciaire agissant en enquête de flagrance, ainsi que des juges d'instruction ; que la rédaction de l'article R. 20-44-9 nouveau doit être aménagé en conséquence ;

Considérant enfin que le texte proposé pour l'article R. 20-44-9 doit, dans l'intérêt même des personnes concernées, prévoir que l'organisme satisfait aux demandes d'informations des services d'urgences habilités par l'autorité publique formulées au titre de leurs missions de la sauvegarde de la vie humaine ;

Est d'avis :

1) De compléter le premier alinéa de l'article R. 10-1 par la phrase suivante : « A ce que ne soient pas mentionnées les données nominatives la concernant dans un annuaire distribué ou diffusé sur un support électronique accessible depuis le territoire d'un État n'assurant pas aux données personnelles une protection équivalente à celle garantie par la loi française. »

De supprimer le deuxième alinéa du même article et de compléter le troisième alinéa par la phrase suivante :

« L'exercice des autres droits est gratuit. »

De procéder aux articles R. 20-44-5 et R. 20-44-7 aux coordinations subséquentes.

2) De rédiger l'article R. 20-44-9 ainsi qu'il suit : «

Article R. 20-44-9 (Sécurité) :

— L'organisme satisfait aux demandes d'informations des autorités habilitées, et notamment aux demandes présentées, dans le cadre de l'exercice de leurs missions de sauvegarde de la vie humaine, par les services d'urgence habilités par l'autorité publique »

II. LA GESTION PERSONNALISEE DE LA CLIENTÈLE

Le souci de présenter une offre commerciale et tarifaire adaptée à chaque client et de réduire les risques économiques a conduit France Télécom à mettre en œuvre depuis 1995, une application de gestion personnalisée de sa clientèle, dénommée « FREGATE » : grâce un identifiant interne unique, tous

les services souscrits par un même abonné sont rassemblés dans un seul traitement qui repose sur la connaissance permanente du solde du compte client ; associé à une « échelle de risques » calculée en fonction des délais de paiements des factures, le traitement « FREGATE » permet un contrôle des débiteurs à la prise de commande, la tenue des comptes différenciés et le recouvrement des créances.

À l'occasion de l'avis favorable rendu par délibération n° 95-006 du 10 janvier 1995 concernant « FREGATE », il convient de rappeler que la CNIL avait pris acte de ce que cette gestion différenciée, dans la mesure où elle s'appuie sur le traitement de données strictement objectives (effectivité et délais des paiements), ne constitue, au regard de l'article 2 de la loi du 6 janvier 1978, qu'une aide à la décision à l'égard des débiteurs défaillants ; qu'enfin, le droit d'accès s'applique à la valeur de l'indicateur résultant des délais écoulés entre la date limite de règlement de la facture et la date effective du paiement. Par ailleurs, la Commission avait clairement indiqué que l'exploitation des données à des fins d'opérations de promotion de produits et services de France Télécom devait s'effectuer dans le respect des listes orange et rouge, la Commission prenant aussi acte de l'existence d'un droit d'opposition spécifique *[cf.* 16e rapport, p. 141).

En 1997, France Télécom a souhaité apporter à son système « FREGATE » des modifications substantielles. Il s'agit en premier lieu d'enrichir systématiquement le fichier des clients d'une information relative au type d'habitat de l'abonné. Cette information résulte d'une classification géo-sociale de l'habitat, établie sur la base de la nature individuelle ou collective de l'habitat, en croisement avec des informations fournies par l'INSEE ayant trait à la sociologie des communes (rurale, urbaine, quartiers résidentiels...). Il ressort de cette typologie vingt catégories principales d'habitat et soixante cinq classes plus fines, entre lesquelles France Télécom entend répertorier l'ensemble de ses clients.

Ainsi, France Télécom espère améliorer l'organisation de ses équipes en cas de dérangements signalés, tout en maintenant le niveau de sécurité de ses personnels ; il s'agit aussi d'optimiser l'offre commerciale et d'adapter les modalités de recouvrement des créances. À cet égard, et bien que la localisation des clients ne constitue qu'un élément d'appréciation parmi d'autres pour définir les modalités de recouvrement des créances, la CNIL a tenu à rappeler que le critère socio-géographique, de nature statistique, n'est absolument pas objectif vis-à-vis d'une personne particulière ; aussi, en cas d'appréciation défavorable, l'abonné doit conserver la faculté de se faire entendre avant toute décision définitive. La Commission a également précisé strictement les conditions d'utilisation de la caractéristique de l'habitat, tout particulièrement dans la perspective où ces informations pourraient être commercialisées dans le cadre des futures activités de cession de listes extraites des annuaires.

Par ailleurs, au titre d'une finalité de son traitement étendue de la gestion interne de ses clients à celle de la distribution de ses produits et services, France

Télécom a proposé d'élargir la liste des destinataires des informations contenues dans « FREGATE » à ses sous-traitants, ainsi qu'à ses éventuels partenaires commerciaux. S'il n'y a pas, sur ce point, d'opposition de principe de la Commission, celle-ci a néanmoins rappelé qu'il ne peut s'agir que d'opérations (études, prospection, distribution) portant exclusivement sur des produits ou des services de France Télécom, au risque d'outrepasser la finalité d'un fichier conçu à des fins de gestion d'un service public, a *fortiori* encore dans une situation de monopole. De plus, France Télécom s'est engagé à ne communiquer d'extraits de son fichier de clientèle que dans le cadre d'un contrat spécifiant les obligations de confidentialité du sous-traitant. Malgré tout, ces extraits de fichiers ne pourront en aucun cas concerner des informations relatives aux factures et à la situation familiale d'un client, qui l'aurait le cas échéant communiquée volontairement.

Enfin, la CNIL a estimé que l'allongement, de deux à dix ans, de la durée de conservation des informations collectées dans le système « FREGATE » se justifiait seulement pour les informations se rapportant à la facturation, à l'exception des numéros appelés par l'abonné qui devront être effacés au plus tard à l'issue des délais prévus par l'article L. 126 du code des postes et télécommunications. En effet, la Commission a relevé que les obligations comptables qui découlent de la transformation de France Télécom en société anonyme ne peuvent en aucun cas concerner l'intégralité des informations traitées, pour lesquelles doit continuer à s'appliquer la durée maximale de deux ans après la clôture du dossier client, c'est-à-dire après paiement de la facture.

En définitive, et sous réserve que le projet d'acte réglementaire soit modifié dans le sens préconisé par la CNIL, un avis favorable a été donné à la modification du traitement « FREGATE ». Par la suite, la CNIL s'est également prononcée favorablement sur d'autres modifications de ce traitement engendrées par l'ouverture du capital de France Télécom, sur la base d'un actionnariat public. En effet, il a été prévu de recourir à « FREGATE », d'une part pour recenser les actionnaires abonnés auprès de France Télécom et, d'autre part, pour gérer les avantages accordés aux abonnés membres du club d'actionnaires.

Délibération n° 97-018 du 11 mars 1997 relative à la demande de modification présentée par France Télécom concernant le traitement automatisé d'informations nominatives destiné à la gestion personnalisée de la clientèle dénommé « FREGATE »

(Demande de modification du dossier n° 355 807)

La Commission nationale de l'informatique et des libertés,

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 2, 15, 26, 27 et 35 ;

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

Vu le décret n° 96-1174 du 27 décembre 1996 approuvant les statuts de France Télécom ;

Vu la délibération n° 95-006 du 10 janvier 1995 portant avis relatif au traitement « FRÉGATE » ;

Vu la décision du 27 janvier 1995 du président du conseil d'administration de France Télécom autorisant la création du traitement automatisé d'informations nominatives relatif à la gestion personnalisée de la clientèle de France Télécom, prise après avis précité de la Commission ;

Vu le projet de décision du président du conseil d'administration de France Télécom destiné à modifier la décision précitée du 27 janvier 1995 ;

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

Considérant que la Commission a été saisie par France Télécom de modifications du traitement relatif à la gestion personnalisée de sa clientèle dénommé « FRÉGATE » ;

Considérant que la finalité actuelle du traitement « FRÉGATE » concerne exclusivement la gestion interne des abonnés de France Télécom effectuée de manière personnalisée et différenciée en fonction des produits et services utilisés ; qu'elle permet l'établissement de la liste des produits et services dont dispose un abonné, la tenue de son compte, l'émission de sa facture et son recouvrement, la gestion des réclamations et du contentieux, la réalisation d'opérations de sondage et l'établissement de statistiques, la réalisation d'opérations d'information et de promotion sur les produits et services commercialisés par France Télécom ;

Sur l'enrichissement du fichier des abonnés par l'indication de la catégorie « géo-sociale » de leur habitat

Considérant que les modifications envisagées concernent tout d'abord l'enrichissement du fichier des abonnés par une information relative à la catégorie « géo-sociale » de l'habitat liée à l'adresse de l'abonné dénommé « téléstyle » ;

Considérant que la typologie des habitats est établie en fonction du caractère individuel ou collectif de l'habitat ainsi que des données statistiques relatives aux tailles des communes et à leur caractère rural ou urbain ainsi qu'au niveau social des communes et des quartiers de résidence calculé à partir des données issues du recensement général de population et établi, conformément à la délibération de la CNIL n° 89-10 du 14 février 1989, pour des zones supérieures à 5000 personnes ;

Considérant que cette typologie conduit à distinguer les zones géographiques selon vingt catégories principales d'habitat et soixante cinq catégories plus fines en fonction de la taille des communes et de leur caractère rural ou urbain, le niveau social des quartiers étant déterminé selon une échelle distinguant cinq niveaux, des quartiers les plus modestes aux quartiers les plus aisés ;

Considérant que chacune de ces catégories constitue un profil « géo-social » que France Télécom entend associer à chacun de ses abonnés en fonction de son adresse ;

Considérant qu'il est envisagé que cette information concoure à la gestion personnalisée et différenciée de la clientèle pour l'adaptation des modalités d'organisation des relèves en cas de dérangements signalés, l'adaptation des modalités de recouvrement de créance du client, et pour l'offre commerciale par France Télécom de ses propres produits et services ;

Considérant qu'il n'est pas illégitime que France Télécom envisage d'utiliser cette information en ce qui concerne l'organisation des déplacements de ses agents pour tenir compte, par exemple, de la distance à parcourir ; qu'il n'est pas davantage illégitime que France Télécom souhaite promouvoir ses produits et services par des actions d'information en direction de ses abonnés en fonction des caractéristiques « géo-sociales » de leur zone géographique d'habitat ainsi que d'autres sociétés commerciales le font d'ores et déjà ; qu'en tout état de cause ce profil « géo-social » associé à une personne constitue une information nominative qui doit être communiquée à la personne concernée lorsqu'elle exerce son droit d'accès en application des articles 34 et suivants de la loi du 6 janvier 1978 ; qu'il y a lieu de relever, en outre, que les abonnés de France Télécom ont un droit d'opposition spécifique aux traitements de leurs données à des fins de prospection commerciale ;

Considérant en revanche, que l'utilisation de cette information « géo-sociale » en matière de modalités de recouvrement des créances, pourrait avoir pour effet d'aboutir à la définition de conduites à tenir, différentes selon des profils statistiques ; que si France Télécom recourt jusqu'à présent en cette matière à un indicateur, cet indicateur repose sur un élément objectif et personnel lié à l'abonné, à savoir le délai écoulé entre la date d'exigibilité d'une facture et la date de son paiement effectif ; qu'il y a lieu de relever que l'adjonction à cet indicateur d'un profil « géo-social » constitue une information statistique sans rapport avec une personne donnée, dont l'utilisation doit être appréciée au regard de l'article 2, alinéa 2 de la loi du 6 janvier 1978 qui indique qu'aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé ; que dans ces conditions il convient que cette information de nature « géo-sociale » ne soit utilisée que comme un élément, parmi d'autres, d'appréciation de la situation de l'intéressé et que, lorsque cette information peut conduire à une décision défavorable à l'égard de l'abonné, ce dernier soit mis en mesure de faire valoir sa situation exacte avant toute décision définitive à son encontre ;

Sur la modification relative aux informations collectées de manière facultative auprès des abonnés

Considérant que l'une des modifications envisagées consiste à collecter de manière facultative auprès des abonnés des informations en vue d'étudier et d'adapter les offres des services et produits de France Télécom ; que ces informations concernent la situation de famille (composition du foyer, âges et activités), le comportement consumériste, selon la catégorie socioprofessionnelle et les revenus, l'utilisation de biens et services autres que ceux

offerts par France Télécom, la préférence du client pour des conseils d'achats ou pour l'affectation d'un interlocuteur privilégié ;

Considérant que cet enrichissement du fichier n'appelle pas d'observation particulière dès lors qu'il est prévu que les personnes sont explicitement informées du caractère facultatif des réponses qui leurs sont demandées, ainsi que des destinataires de ces informations, ce que France Télécom a l'obligation de faire en application de l'article 27 de la loi ; qu'à cet égard il conviendra que France Télécom prenne toute mesure afin d'informer ses abonnés, lors de la collecte de ces informations supplémentaires, des catégories de destinataires qui pourraient en avoir connaissance ;

Sur l'ajout de la mention du mandataire de l'abonné

Considérant que l'enrichissement du fichier de clientèle de la mention du mandataire éventuel du client n'appelle pas d'observation particulière ;

Sur l'élargissement de la liste des destinataires des informations aux sous-traitants de France Télécom ainsi qu'à ses partenaires commerciaux

Considérant que France Télécom envisage de communiquer à des sous-traitants des extraits du fichier de clientèle dans le cadre de contrats spécifiant les obligations de confidentialité du sous traitant ; que les extraits de fichiers ne concernent en aucun cas les informations relatives aux factures et à la situation familiale du client ;

Considérant que les opérations ainsi réalisées seront effectuées pour le compte de France Télécom ; qu'une telle utilisation est possible dès lors que l'abonné ne s'y est pas opposé et que cette prospection concerne exclusivement des produits ou services de France Télécom ;

Considérant que, par ailleurs, France Télécom envisage, dans le but de diversifier les modes de commercialisation de ses produits, de passer des accords avec des partenaires commerciaux, distributeurs, courtiers et agents commerciaux ;

Considérant que la communication d'informations relatives aux abonnés de France Télécom à ces partenaires dépendra de l'objet du partenariat et sera précisée dans le contrat de partenariat ; que ces communications pourraient concerner, selon le partenariat, tout ou partie des informations relatives à l'identité de l'abonné et de son mandataire, à ses adresses, ses numéros de téléphones, les téléstyles correspondant aux adresses, les informations que l'abonné aura communiquées à France Télécom de manière facultative, la liste des produits France Télécom qu'il détient ;

Considérant que la communication d'informations issues du fichier des abonnés à des sous — traitants ou partenaires commerciaux, à des fins de prospection ne portant pas exclusivement sur des produits ou services de France Télécom, excéderait la finalité du fichier constitué aux fins de gestion d'un service public, et en l'état sous monopole ; qu'une telle communication appellerait dès lors une objection de principe ;

Sur l'allongement de la durée de conservation des informations

Considérant que France Télécom souhaite allonger la durée de conservation des informations collectées et traitées dans le cadre du système « FRÉGATE » de deux ans à dix ans, faisant valoir que ses obligations comptables découlant de l'article 16 du code de commerce le justifie ; Considérant qu'un tel allongement de la durée de conservation ne se trouve justifié que pour les informations qui se rapportent directement et exclusivement à la facturation, à l'exception des numéros appelés par l'abonné qui ne doivent pas être conservés au-delà des délais prévus par l'article 126 du code des postes et télécommunications ; que les informations relatives aux autres fonctions du traitement ne pourront pas être conservées au-delà d'un délai de deux ans ;

Émet un avis favorable à la mise en œuvre du traitement sous réserve que :

— L'article 3 du projet de décision soit complété par un deuxième alinéa rédigé ainsi qu'il suit :

« Il est ajouté, après le premier alinéa de l'article 2 de cette décision, un deuxième alinéa ainsi rédigé :

« Toutefois, la typologie de l'habitat n'est utilisée que dans les cas et aux conditions suivantes :

- en cas de nécessité d'un déplacement sur le lieu de résidence de l'abonné,
- en cas de prospection commerciale, sous réserve que l'abonné ne s'y soit pas opposé,
- en cas d'impayés, sous la réserve que l'abonné, dans le cas où la prise en compte de cette information conduirait à une décision défavorable à son égard, soit mis en mesure de faire valoir sa situation exacte avant toute décision définitive à son encontre ».

- L'article 4 du projet de décision soit rédigé ainsi qu'il suit :

« Il est ajouté à l'article 2 de cette décision un troisième alinéa ainsi rédigé : « La durée maximale de conservation des informations est de deux ans après la clôture du dossier client, à l'exception des informations qui se rapportent directement et exclusivement à la facturation qui sont conservées pendant une durée maximale de dix ans. Les numéros appelés par l'abonné ne sont pas conservés au-delà des délais prévus par l'article L. 126 du code des postes et télécommunications. »

— L'article 5 du projet de décision soit complété par la phrase suivante : « Cet article est par ailleurs complété par la phrase suivante :

« Toutefois, aucune information issue du fichier des abonnés n'est communiquée à des sous-traitants ou partenaires commerciaux à des fins de prospection ne portant pas exclusivement sur des produits ou services de France Télécom. »

Délibération n° 97-089 du 18 novembre 1997 concernant une demande d'avis portant modification du traitement d'informations nominatives « FRÉGATE » relatif à la gestion personnalisée de la clientèle de France Télécom

(Demande d'avis n° 355 807)

La Commission nationale de l'informatique et des libertés,

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

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

Vu le code de procédure pénale ;

Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ;

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation de télécommunications et le décret n° 96-1225 du 27 décembre 1996 portant approbation du cahier des charges de France Télécom ;

Vu la loi n° 96-660 du 26 juillet 1996 relative à l'entreprise nationale France Télécom et le décret n° 96-1174 du 27 décembre 1996 approuvant les statuts de France Télécom et portant diverses dispositions relatives au fonctionnement de l'entreprise nationale ;

Après avoir entendu Monsieur Marcel Pinet, en son rapport et Madame Cnarlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Considérant que France Télécom a adressé à la Commission une demande d'avis portant modification du traitement relatif à la gestion personnalisée de la clientèle de France Télécom destinée à tenir compte de l'échange d'informations nominatives opéré entre ce traitement et le système d'information des actionnaires de France Télécom ; que le système d'information des actionnaires de France Télécom a fait l'objet des formalités préalables de déclaration d'un traitement d'informations nominatives auprès de la Commission en application de l'article 16 de la loi du 6 janvier 1978 ;

Considérant que France Télécom souhaite offrir des avantages particuliers aux abonnés membres de son club d'actionnaires ; qu'à cette fin, l'opérateur souhaite recenser, parmi l'ensemble de son actionnariat, les personnes qui sont également abonnées à ses services ; que, dès lors un échange d'informations nominatives entre le système d'information des actionnai/es (SIA) et le traitement de gestion des abonnés de France Télécom (FRÉGATE) est effectué ; que le traitement FRÉGATE fournira au SIA, le cas échéant, le numéro de téléphone des abonnés actionnaires, ainsi que la mise à jour des nom, prénoms et adresse de ces personnes ;

Considérant que les données relatives aux avantages offerts aux abonnés membres du club FT seront transmises par le SIA au traitement FRÉGATE qui contrôlera la régularité du règlement des factures téléphoniques de ces abonnés afin de déterminer les avantages auxquels ils peuvent bénéficier ; qu'en retour, le traitement FRÉGATE fournira au SIA le montant des avantages effectivement accordés à chaque abonné membre du club FT ;

Considérant qu'il convient que les fonctionnalités nouvelles qu'implique la mise en œuvre du SIA pour le traitement FRÉGATE soient prises en compte dans l'acte réglementaire relatif au traitement FRÉGATE ;

Émet un avis favorable au projet de modification de l'acte réglementaire relatif au traitement FRÉGATE de gestion différenciée de la clientèle de France Télécom.

III. LE TRAITEMENT « MINITELNET »

France Télécom a présenté à la CNIL un service de messagerie électronique dénommé « Minitelnet », qui rend accessible la messagerie électronique de l'Internet, par le biais du réseau Télétel en ce qui concerne la France ou par le biais du réseau téléphonique international pour l'étranger. L'inscription au « 3615 Minitelnet » permet de disposer d'une adresse de messagerie électronique et d'échanger des messages avec des correspondants disposant d'une boîte aux lettres électronique Internet (mél ou « mail »). En pratique, le titulaire d'une boîte aux lettres « Minitelnet » peut, après avoir composé un mot de passe, consulter ou supprimer les messages qu'il a émis ou reçus, et gérer un répertoire d'adresses.

La sécurité du service repose d'abord sur l'authentification du titulaire d'une boîte aux lettres grâce à son adresse électronique Internet et son mot de passe, une déconnexion du service intervenant automatiquement après trois tentatives erronées pour accéder à une boîte aux lettres. Afin d'éviter l'envoi intempestif de messages à des fins de prospection commerciale via le service « Minitelnet », il a été prévu que le nombre de destinataires d'un même message ne pourrait excéder cent. Enfin, le contrat d'utilisation du service, expédié par voie postale à l'adresse indiquée lors de l'inscription « en ligne » au service, confirme à l'utilisateur l'ouverture d'une boîte aux lettres à son nom et lui communique son numéro confidentiel de boîte.

Lorsque l'inscription à « Minitelnet » est effectuée par un tiers, cette faculté étant effectivement offerte, la CNIL a demandé un certain nombre de garanties supplémentaires. Ainsi, la CNIL a exigé qu'aucun message ne puisse être adressé au titulaire d'une boîte tant que ce dernier n'a pas accompli la procédure d'ouverture décrite ci-dessus. En outre, la Commission a rappelé que les personnes pour le compte desquelles une boîte aux lettres est créée, doivent pouvoir s'opposer à leur inscription en se connectant au service afin de fermer leur boîte ou en s'adressant par téléphone ou par courrier au numéro ou à l'adresse indiqués dans la lettre les informant de leur inscription au service. Dans tous les cas, il est prévu que toute boîte inutilisée sera fermée d'autorité par France Télécom, au terme d'un délai de deux cents jours.

France Télécom a prévu, en contrepartie de la gratuité de l'inscription au service, de céder à des société tierces, en vue de prospection commerciale, les informations relatives aux titulaires des boîtes. Cependant, en concertation

avec la CNIL, France Télécom s'est engagé à ce qu'une page-écran d'accès au service « Minitelnet » informe les personnes des droits qui leurs sont ouverts sur le fondement de la loi « Informatique et Libertés », notamment le droit d'opposition à ce que leurs données soient cédées à des tiers ; la Commission a également souligné que le contrat devait mentionner ces informations. Enfin, dans l'hypothèse des boîtes ouvertes par des tiers (environ 10 %), la Commission a tenu à rappeler qu'en aucun cas, le titulaire d'une boîte qui ne l'a jamais ouverte au moyen de son code confidentiel, ne pourra voir ses coordonnées cédées à des tiers à des fins commerciales ; en effet, la CNIL a estimé que le titulaire de la boîte n'a dès lors pas été pleinement informé de ses droits au regard de la législation sur la protection des données personnelles.

Délibération n° 97-050 du 24 juin 1997 relative à une demande d'avis présentée par France Télécom concernant un traitement automatisé d'informations nominatives dénommé « Minitelnet »

(Demande d'avis n° 505 945)

La Commission nationale de l'informatique et des libertés,

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

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

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

Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ;

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation de télécommunications ;

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

Considérant que la Commission a été saisie d'une demande d'avis présentée par France Télécom relative à un traitement automatisé d'informations nominatives concernant la mise en place d'un service de messagerie électronique accessible en France par le biais du réseau Télétel et dont la finalité principale est de permettre l'accès à la messagerie électronique sur Internet ; que ce service est également accessible à partir de l'étranger par l'intermédiaire du réseau téléphonique international et des services d'accès au réseau Télétel commercialisés par France Télécom ; Considérant que ce service, dénommé « 3615 Minitelnet», permet à un utilisateur d'ouvrir et de disposer d'une boîte aux lettres électronique Internet et d'échanger des messages avec des correspondants disposant d'une boîte aux lettres électronique Internet ; que l'inscription à ce service est gratuite ;

Considérant que le titulaire de la boîte aux lettres électronique peut consulter les messages qu'il a émis, consulter et supprimer les messages qu'il a reçus et gérer le répertoire d'adresses et les listes de diffusion qu'il aura constitués ;

Considérant que ce service ne permet ni l'envoi, ni la réception de fichiers joints à un message ; qu'en outre, dans le souci d'éviter le détournement du service à des fins de prospection commerciale, il est techniquement impossible que le nombre de destinataires d'un même message, lors d'un même envoi, excède cent ;

Considérant que, pour accéder à sa boîte aux lettres, le titulaire doit composer un mot de passe constitué par une suite de quatre à dix caractères alphanumériques de son choix, l'authentification du titulaire d'une boîte aux lettres reposant sur l'association de son adresse électronique Internet et de son mot de passe ; que le titulaire peut changer à tout moment de mot de passe ; qu'en outre, tout utilisateur sera automatiquement déconnecté du service après trois tentatives erronées pour accéder à une boîte aux lettres ;

Considérant, par ailleurs, que dans un souci d'identification de l'émetteur d'un message, le service Minitelnet transmet systématiquement aux destinataires des messages émis, le nom et le prénom du titulaire de la boîte aux lettres émettrice ;

Considérant qu'une lettre de bienvenue accompagnée du contrat d'utilisation du service est expédiée par voie postale à l'adresse indiquée lors de l'inscription « en ligne » au service ; que le titulaire d'une boîte aux lettres est informé de l'ouverture d'une boîte aux lettres à son nom et de son numéro confidentiel de boîte, composé de sept chiffres ;

Considérant que le service Minitelnet permet d'ouvrir et de mettre à disposition d'un tiers une boîte aux lettres électronique Internet ; que dans ce cas, le numéro confidentiel de boîte aux lettres est adressé à la personne pour le compte de laquelle une boîte aux lettres est créée ; que cette personne peut s'opposer à son inscription en se connectant au service Minitelnet et en fermant sa boîte, ou en s'adressant par téléphone ou par courrier au numéro ou à l'adresse indiqués dans la lettre de bienvenue ; qu'en outre, lorsque le courrier par lequel le numéro de boîte aux lettres est notifié au titulaire de la boîte sera retourné au service Minitelnet avec la mention « NPAI » (n'habite pas à l'adresse indiquée), la boîte aux lettres électronique du titulaire sera immédiatement supprimée, afin de prévenir dans les plus brefs délais, toute possibilité d'usurpation d'identité du fait de l'inscription « en ligne » ;

Considérant que les informations traitées sont le nom du titulaire de la boîte aux lettres, son ou ses prénom (s), son adresse postale, son adresse et son numéro de boîte aux lettres électronique Internet, son mot de passe, les messages dont il est destinataire ou émetteur et, de façon facultative, son numéro de téléphone ;

Considérant que ces informations sont conservées jusqu'à la fermeture d'une boîte aux lettres ; que toute boîte aux lettres qui n'aura pas été utilisée pendant une période de deux cents jours sera supprimée d'office par France Télécom ;

Considérant que les destinataires de ces informations sont le titulaire de la boîte aux lettres et, pour les actes de gestion du service, les agents habilités de France Télécom, dont il y a lieu de relever qu'ils ne pourront en aucun cas avoir accès au contenu du message ;

Considérant, en outre, que France Télécom envisage de céder à des sociétés tierces les informations nominatives relatives au titulaire de la boîte aux

lettres communiquées lors de son inscription au service Minitelnet ; qu'il s'agit du nom, du ou des prénom(s), de l'adresse et du numéro de téléphone ;

Considérant que les titulaires des boîtes aux lettres ont la possibilité de refuser que les informations nominatives les concernant soient cédées à des tiers ; qu'à cette fin, une page écran, accessible par une rubrique intitulée « Informatique et Libertés », comporte les informations prévues par l'article 27 de la loi du 6 janvier 1978, et la mention suivante :

« Vous pouvez vous opposer à la cession à des tiers, par France Télécom, des données vous concernant, en écrivant au service Minitelnet de France Télécom ou en envoyant un message à l'adresse électronique : serviceclient-minitel. net. »

Considérant que les personnes inscrites au service Minitelnet sont également informées par le contrat qui leur est expédié à la suite de leur inscription, des droits dont elles disposent, grâce à une clause identique à celle figurant « en ligne » sur le service Minitelnet ;

Considérant que le contrat précise, en outre, que la remise effective, l'intégrité, l'authenticité et la confidentialité des messages échangés par le service Minitelnet n'est pas garantie en raison du caractère non sécurisé du réseau Internet, et que les titulaires d'une boîte aux lettres sont responsables du contenu et de la nature des messages et des données qu'ils peuvent échanger sur le service Minitelnet ;

Considérant, cependant, qu'il convient que soit évitée la situation dans laquelle le titulaire d'une boîte aux lettres créée à l'initiative d'un tiers puisse recevoir des messages, sans avoir préalablement accompli la procédure nécessaire à l'ouverture de sa boîte ; qu'il convient également, qu'en aucun cas les données nominatives concernant le titulaire d'une boîte aux lettres créée par un tiers ne puissent être cédées avant que le titulaire de la boîte aux lettres ait volontairement accompli la procédure d'ouverture de sa boîte ;

Considérant que les présentes recommandations ont paru nécessaires à la protection des données personnelles et des personnes elles-mêmes dans la mise en oeuvre de services de ce type ;

Considérant que France Télécom envisage de réaliser un annuaire des adresses Minitelnet, l'inscription dans cet annuaire ne pouvant se faire qu'à la demande du titulaire d'une boîte électronique du service Minitelnet ; que si ce projet devait être mis en œuvre, il conviendrait que France Télécom saisisse la Commission d'une demande d'avis modificative ;

Émet un avis favorable au projet de décision du président du conseil d'administration de France Télécom, sous réserve qu'il soit complété par un alinéa ainsi rédigé :
« En aucun cas, Te titulaire d'une boîte aux lettres créée, à l'initiative d'un tiers ne pourra recevoir des messages s'il n'a ouvert la boîte ainsi créée au moyen du numéro confidentiel qui lui a été attribué. En aucun cas, le titulaire d'une boîte aux lettres créée à l'initiative d'un tiers ne pourra voir cédées les coordonnées communiquées lors de son inscription s'il n'a ouvert la boîte aux lettres ainsi créée, au moyen du numéro confidentiel qui lui a été attribué. »

IV. LE SERVICE DE PRÉSENTATION DU NUMÉRO APPELANT

En septembre 1997, France Télécom a ouvert au public un service de présentation du numéro de téléphone de la ligne appelante, qui a reçu un avis favorable de la CNIL par délibération n° 96-011 du 12 mars 1996 (cf. 17e rapport, p. 362). À cette occasion, la CNIL avait rappelé, d'une part que les abonnés doivent être parfaitement informés de la possibilité de s'opposer gratuitement et à tout moment à la divulgation de leur numéro et d'autre part, l'interdiction absolue de constituer, à l'insu des personnes, des fichiers de numéros appelants.

Dès lors, a été aménagée la possibilité pour les nouveaux abonnés, de manifester lors de la souscription du contrat leur refus permanent de transmission de leur numéro de ligne, tandis qu'un appel gratuit au numéro vert n° 0800 803 800 a été mis en place entre les mois de juillet et décembre 1997 pour les anciens abonnés qui souhaiteraient opter pour le secret permanent. Depuis cette date, les personnes peuvent s'adresser à leur agence commerciale pour manifester leur refus permanent de la transmission de leur numéro à leur correspondant. Par ailleurs, les abonnés qui n'auraient pas eu recours à cette option, ont la possibilité de choisir, également sans frais, le secret appel par appel à partir de leur terminal. Ainsi, deux modes de secret sont mis gratuitement à la disposition des abonnés, soit le secret permanent du numéro de leur ligne, soit le secret appel par appel, en composant le 3651 avant les dix chiffres du numéro appelé. Les personnes qui souhaitent que soit présenté sur leur terminal téléphonique le numéro de la ligne appelante, doivent souscrire un abonnement payant auprès de France Télécom et, si elles ne disposent pas d'un terminal doté d'un écran, acquérir un boîtier spécial permettant l'affichage des numéros.

Néanmoins, la CNIL a reçu des plaintes relatives soit au principe même de ce service, soit aux difficultés rencontrées par les abonnés pour exercer le droit au secret permanent et gratuit. Aussi, à la demande de la CNIL, France Télécom a pris les mesures utiles qui ont permis d'établir la transparence et l'effectivité de l'information donnée aux abonnés.

Par ailleurs, la CNIL s'est inquiétée de l'utilisation qui pourrait être faite des fonctions disponibles sur les appareils téléphoniques récents, qui permettent l'enregistrement des derniers numéros appelants. À cet égard, France Télécom a précisé que sa prestation était limitée à la seule transmission du numéro sur le poste de l'appelé et n'emportait aucune conservation des informations, et ce conformément à ce que la CNIL avait préconisé. Il demeure que le contrat d'abonnement au service de présentation du numéro enjoint au souscripteur de ne pas constituer de fichiers de numéros appelants, un responsable de France Télécom ayant précisé qu'il serait toujours possible pour l'opérateur de résilier unilatéralement l'abonnement d'une personne qui contreviendrait aux clauses du contrat. Cette question prend une dimension particulière dans le cadre du développement à grande échelle des services d'annuaire inversé en France.

ANNEXES

Annexe 1

Composition de la Commission au 1er mai 1998

Président : **Jacques FAUVET**

Vice-président délégué : **Michel BENOIST,** conseiller-maître honoraire à la Cour des comptes

Vice-président : **Raymond FORNI,** député du Territoire de Belfort, maire de Delle

Commissaires :

Michel BERNARD, président de section honoraire au Conseil d'État
Hubert BOUCHET, membre du Conseil économique et social
Thierry CATHALA, conseiller-doyen honoraire à la Cour de cassation
Noël CHAHID-NOURAـ conseiller d'État
Gérard GOUZES, député du Lot-et-Garonne, maire de Marmande
Isabelle JAULIN, avocat à la cour
Jean-Pierre MICHEL, député de Haute-Saône, maire d'Héricourt
Marcel PINET, conseiller d'État honoraire
Jean-Marie POIRIER, conseiller d'État honoraire, sénateur du Val-de-Marne, maire de Sucy-en-Brie
Charles RENARD, président de chambre à la Cour des comptes
Jacques RIBS, conseiller d'État honoraire
Pierre SCHAPIRA, membre du Conseil économique et social
Alex T-RK, 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

Annexe 2

Répartition des secteurs d'activité au 1er mai 1998

Michel BENOIST : banque (sauf Banque de France), segmentation comportementale bancaire, banque à domicile, présidence du collège des commissaires habilités à exercer le droit d'accès indirect.

Michel BERNARD : enseignement public et privé, partis politiques, marketing politique, suivi du contentieux administratif, droit d'accès indirect. **Hubert BOUCHET :** recrutement, emploi, formation, élections professionnelles. **Thierry CATHALA :** trésor, comptabilité publique, fiscalité locale, enquêtes fiscales, douanes, répression des fraudes, droit d'accès indirect.

Noël CHAHID-NOURAJ : Banque de France, crédit à la consommation, nouveaux modes de paiement (hors crédit et Internet), droit d'accès indirect. **Raymond FORNI :** police nationale, gendarmerie nationale, police municipale, renseignement militaire et civil, service national, affaires étrangères. **Gérard GOUZES :** justice (autorité judiciaire, justice administrative, professions judiciaires), autorités administratives indépendantes, archives nationales. **Isabelle JAULIN :** culture, jeunesse et sport, tourisme, transport, équipement, logement, immobilier, environnement, industrie, énergies, agriculture. **Jean-Pierre MICHEL :** santé (gestion hospitalière, des cabinets médicaux et paramédicaux, médecine du travail, médecine préventive). **Marcel PINET :** télécommunications et réseaux, dont Internet, participation aux groupes de travail internationaux dans ce domaine (GERI et groupe dit « de Berlin »), représentation de la CNIL au groupe européen de suivi de la transposition de la directive (groupe dit « de l'article 29 »), poste, droit d'accès indirect. **Jean-Marie POIRIER :** recherche en santé et sciences sociales (dont INED). **Charles RENARD :** enquêtes statistiques mises en œuvre par l'INSEE (dont recensement général de la population), sondages, droit d'accès indirect.

Jacques RIBS : assurance, marketing, commerce dont commerce électronique, artisanat, renseignement commercial, recouvrement de créances, bourse, droit d'accès indirect.

Pierre SCHAPIRA : aide sociale, revenu minimum d'insertion, collectivités locales (gestion des administrés).

Alex T-RK : presse, églises, associations, syndicats, coopération européenne et internationale en matière de police, de justice et de douanes.

Maurice VIENNOIS : sécurité sociale, assurance vieillesse, assurance maladie, allocations familiales, mutuelles, droit d'accès indirect.

Annexe 3

Organisation des services

Président : **Jacques FAUVET**

Secrétaire général chargé des affaires juridiques : **Joël BOYER,** magistrat

Secrétaire général adjoint chargé de l'administration et de la communication **Loïc ROUSSEAU,** chargé de mission

Annexe 4

Liste des délibérations adoptées en 1997

Les délibérations sont publiées dans les chapitres du rapport, à la suite des commentaires qui les évoquent. 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, après abonnement auprès de l'Européenne de Données (base DIVA) ou de la société LEXIS (base AUTOAD).

Nature-numéro date	Objet
97-001 14 janvier 1997 [cf. Troisième partie p. 298)	Délibération portant avis sur le projet d'acte réglementaire présenté par l'ACOSS concernant la modification du traitement relatif à la gestion de la déclaration unique à l'embauche. (Demande d'avis n° 409 224)
97-002 14 janvier 1997 (cf. Troisième partie p. 228)	Délibération portant avis sur un projet d'acte réglementaire présenté par la Caisse nationale d'assurance maladie des travailleurs salariés relatif à un modèle type de traitement automatisé d'informations nominatives dénommé « PROGRES » ayant pour finalité d'assurer le remboursement des prestations. (Demande d'avis n° 435 217)
97-003 14 janvier 1997	Délibération décidant d'un contrôle sur place.
97-004 21 janvier 1997 (cf. Troisième partie p. 170)	Délibération relative à la demande d'avis du ministère de la Justice portant création d'un modèle type de traitement ayant pour objet la gestion des visites en établissement pénitentiaire des familles des détenus. (Demande d'avis n° 451 142)
97-005 21 janvier 1997 (cf. Première par ie p. 17)	Délibération concernant les traitements automatisés d'informations nominatives relatifs à la gestion du patrimoine immobilier à caractère social. (Norme simplifiée n° 20)
97-006 4 février 1997 (cf. Troisième partie p. 249)	Délibération portant avis sur la demande présentée par le conseil général du Rhône et concernant la gestion informatisée de l'aide sociale à l'enfance et de l'action sociale de terrain (ANIS-ASE). (Demande d'avis n° 496 142)

Nature-numéro date	Objet
97-007 4 février 1997	Délibération décidant d'un contrôle sur place.
97-008 4 février 1997 (cf. Deuxième par ie p. 98)	Délibération portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel.
97-009 4 février 1997 (cf. Deuxième par ie p. 86)	Délibération relative à la demande d'avis du Service d'information du Gouvernement concernant le traitement d'informations nominatives opéré dans le cadre du site Internet du Premier ministre et du Gouvernement. (Demande d'avis n° 483 293)
97-010 4 février 1997 (cf. Troisième partie p. 303)	Délibération portant avis sur le projet de décret d'application de l'article L. 35-4 du code des postes et télécommunications relatif à l'annuaire universel.
97-011 4 février 1997	Délibération portant adoption d'un formulaire de demande d'autorisation d'un traitement automatisé d'informations nominatives ayant pour finalité la recherche médicale.
97-012 18 février 1997 (cf. Première par ie p. 55)	Délibération portant recommandation relative aux bases de données comportementales sur les habitudes de consommation des ménages constituées à des fins de marketing direct.
97-013 18 février 1997 {cf. Troisième partie p. 269)	Délibération portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives relatif au rapprochement des listes électorales de Guadeloupe avec le fichier électoral de l'INSEE. (Demande d'avis n° 496 735)
97-014 18 février 1997	Délibération décidant d'un contrôle sur place.
97-015 18 février 1997	Délibération décidant d'un contrôle sur place.
97-016 4 mars 1997 (cf. Troisième partie p. 195)	Délibération portant avis sur le projet de décision présenté par la Caisse centrale de mutualité sociale agricole concernant un modèle type de traitement de gestion des services de médecine du travail des caisses de mutualité sociale agricole. (Demande d'avis n° 466 599)

Nature-numéro date	Objet
97-017 11 mars 1997 (cf. Deuxième partie p. 94)	Délibération portant avis sur la demande présentée par la CNAVTS et concernant une expérimentation de transfert de données sociales par le réseau Internet (TDS-INTERNET).
97-018 11 mars 1997 (cf. Troisième partie p. 309)	Délibération relative à la demande de modification présentée par France Télécom concernant le traitement automatisé d'informations nominatives destiné à la gestion personnalisée de la clientèle dénommé « FREGATE ». (Demande de modification du dossier n° 355 807)
97-019 25 mars 1997	Délibération décidant d'un contrôle sur place.
97-020 25 mars 1997	Délibération portant avis sur un projet d'arrêté modificatif présenté par le ministère de l'Intérieur concernant la délivrance des certificats de non-gage et de non-opposition au transfert de carte grise.
97-021 25 mars 1997 (cf. Troisième partie p. 157)	Délibération portant avis sur un projet d'article L. 115-8 du code de la sécurité sociale.
97-022 1er avril 1997 (cf. Troisième partie p. 245)	Délibération portant avis sur la demande présentée conjointement par le conseil général des Alpes-Maritimes et la préfecture des Alpes-Maritimes et concernant la mise en œuvre d'un traitement automatisé de données nominatives relatif à la gestion des commissions locales d'insertion et le suivi de l'insertion. (Demande d'avis n° *457* 715)
97-023 1er avril 1997 (cf. Troisième partie p. 198)	Délibération relative à un projet d'arrêté présenté par le ministère du Travail et des Affaires sociales relatif à l'informatisation des déclarations obligatoires de sida avéré.
97-024 1er avril 1997 (cf. Troisième partie p. 199)	Délibération relative à un projet d'arrêté présenté par la direction générale de la santé du ministère du Travail et des Affaires sociales concernant la mise en œuvre, dans chaque direction départementale des affaires sanitaires et sociales d'un traitement national de données indirectement nominatives issues des déclarations obligatoires de sida détenues par le RNSP. (Demande d'avis n° 520 468)

Nature-numéro date	Objet
97-025 1er avril 1997 (cf. Troisième partie p. 200)	Délibération relative à un projet d'acte réglementaire présenté par le réseau national de santé publique concernant un traitement automatisé d'informations indirectement nominatives ayant pour finalité la surveillance de l'épidémie de sida à partir des déclarations obligatoires des cas de sida. (Demande d'avis n° 494 968)
97-026 1er avril 1997 (cf. Troisième partie p. 139)	Délibération relative à la visite sur place effectuée le 7 janvier 1997 à la direction de la construction et du logement de la mairie de Paris.
97-027 1er avril 1997 (cf. Troisième par ie p. 270)	Délibération portant avis favorable à la mise en œuvre, par l'INSEE, du recensement général de la population (RGP) à Mayotte. (Demande d'avis n° 505 596)
97-028 1er avril 1997 (cf. Troisième partie p. 272)	Délibération portant avis sur le projet de décret, présenté par l'INSEE, portant application des dispositions de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978, au traitement automatisé d'informations nominatives mis en œuvre à l'occasion du recensement général de la population (RGP) à Mayotte. (Demande d'avis n° 505 596)
97-029 22 avril 1997	Délibération décidant d'un contrôle sur place.
97-030 6 mai 1997 (cf. Troisième partie p. 251)	Délibération portant avis sur la demande présentée par le conseil général du Tarn et concernant l'informatisation de l'aide sociale générale départementale « PHILEAS-ASG ». (Demande d'avis n° 491 791)
97-031 6 mai 1997	Délibération décidant d'un contrôle sur place.
97-032 6 mai 1997 (cf. Deuxième par ie p. 88)	Délibération relative à la demande d'avis présentée par le Premier ministre concernant un modèle type de traitements d'informations nominatives opérés dans le cadre d'un site Internet ministériel. (Demande d'avis n° 520 219)

Nature-numéro date	Objet
97-033 6 mai 1997 [cf. Troisième partie p. 167)	Délibération portant avis sur la déclaration de modification du traitement « CARTECOLE », présentée par la mairie de Paris. (Demande d'avis n° 391 900)
97-034 6 mai 1997	Délibération décidant d'un contrôle sur place.
97-035 6 mai 1997	Délibération décidant d'un contrôle sur place.
97-036 27 mai 1997 (cf. Troisième partie p. 172)	Délibération portant avis sur le modèle type de traitement présenté par le ministère de la Justice concernant la gestion des contrôles d'accès des personnels dans les établissements pénitentiaires. (Demande d'avis n° 451 139)
97-037 27 mai 1997 (cf. Troisième partie p. 291)	Délibération portant avis sur un modèle type présenté par la Caisse des dépôts et consignations dénommé « PRORISQ » et ayant pour finalité le recueil des données concernant les risques professionnels dans les fonctions publiques territoriale et hospitalière. (Demande d'avis n° 485 469)
97-038 27 mai 1997	Délibération décidant d'un contrôle sur place.
97-039 27 mai 1997	Délibération décidant d'un contrôle sur place.
97-040 27 mai 1997	Délibération décidant d'un contrôle sur place.
97-041 27 mai 1997	Délibération portant adoption du 17e rapport d'activité de la CNIL.
97-042 27 mai 1997 (cf. Troisième partie p. 204)	Délibération portant autorisation de mise en œuvre par l'INSERM (unité 170) d'un traitement automatisé d'informations nominatives ayant pour finalité une étude épidémiologique de la mortalité des travailleurs exposés aux fumées de bitume. (Demande d'autorisation n° 518 473)

Nature-numéro date	Objet
97-043 27 mai 1997	Délibération décidant d'un contrôle sur place.
97-044 10 juin 1997 [cf. Troisième partie p. 288)	Délibération portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des agents par empreintes digitales. (Demande d'avis n° 495 531)
97-045 10 juin 1997 (cf. Troisième partie p. 289)	Délibération portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des convoyeurs de fonds à l'aide de bornes d'authentification vidéo. (Demande d'avis n° 495 537)
97-046 10 juin 1997 [cf. Troisième partie p. 266)	Délibération portant avis sur la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives ayant pour objet la conduite d'une étude statistique sur l'évolution de la participation électorale en 1997. (Demande d'avis n° 368 533)
97-047 10 juin 1997 [cf. Troisième partie p. 214)	Délibération portant avis sur un projet de décret autorisant l'accès aux données relatives au décès des personnes figurant au répertoire national d'identification des personnes physiques dans le cadre des recherches dans le domaine de la santé.
97-048 10 juin 1997 [cf. Troisième partie p. 193)	Délibération portant avis sur le projet d'arrêté présenté par le ministère de l'Intérieur autorisant la création d'un modèle national de traitement automatisé d'informations nominatives relatif à la gestion des services de médecine de prévention. (Demande d'autorisation n° 517 344)
97-049 24 juin 1997 [cf. Deuxième partie p. 105)	Délibération portant avis sur la mise en oeuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le centre hospitalier d'Annecy et certains médecins de ville. (Demande d'avis n° 453 828)
97-050 24 juin 1997 [cf. Troisième partie p. 316)	Délibération relative à une demande d'avis présentée par France Télécom concernant un traitement automatisé d'informations nominatives dénommé « Minitelnet ». (Demande d'avis n° 505 945)

Nature-numéro date	Objet
97-051 30 juin 1997 [cf. Deuxième partie p. 92)	Délibération concernant une demande d'avis présentée par la mairie de Paris relative à un traitement d'informations nominatives mis en œuvre dans le cadre du site Internet de la ville de Paris. (Demande d'avis n° 517 197)
97-052 30 juin 1997 (cf. Troisième partie p. 242)	Délibération portant avis sur la demande présentée par la Caisse nationale des allocations familiales relative au fichier national de contrôle des bénéficiaires du revenu minimum d'insertion. (Demande d'avis n° 495 432)
97-053 30 juin 1997	Délibération décidant d'un contrôle sur place.
97-054 30 juin 1997 [cf. Troisième partie p. 175)	Délibération portant avis conforme sur un projet de décret du ministre de la Justice portant application des dispositions de 'article 31, troisième alinéa, de la loi du 6 janvier 1978 au traitement automatisé de gestion centralisée de la population pénale mis en œuvre par la direction de l'administration pénitentiaire.
97-055 30 juin 1997 [cf. Troisième partie p. 177)	Délibération portant avis sur un projet d'arrêté du ministre de a Justice relatif à la création d'un traitement automatisé de données nominatives destiné à assurer la gestion centralisée de a population pénale (« GCPP »). (Demande d'avis n° 497 156)
97-0 56 30 juin 1997	Délibération portant avis sur un projet d'arrêté du ministre de la Justice concernant la création d'un modèle type de traitement de gestion régionale de la population pénale (« GRPP »). (Demande d'avis n° 492 435)
97-057 8 juillet 1997 [cf. Première partie p. 46)	Délibération relative à une proposition de décret portant application des dispositions de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978 au fichier mis en œuvre par la ville de Paris aux fins de recenser les biens immobiliers dont ont été spoliées des personnes considérées comme juives par les autorités de Vichy et d'identifier leurs ayants droit.

Nature-numéro date	Objet
97-058 8 juillet 1997 (cf. Première par ie p. 47)	Délibération portant avis sur un projet d'arrêté du maire de Paris relatif à la création d'un traitement destiné à rechercher les conditions dans lesquelles des biens immobiliers auraient été acquis par la ville de Paris, à la suite de spoliations de personnes considérées comme juives par le régime de Vichy. (Demande d'avis n° 520 306)
97-059 8 juillet 1997 (cf. Troisième partie p. 164)	Délibération portant avis sur la déclaration de modification du traitement « scolarité » présentée par le ministère de l'Éducation nationale, de la Recherche et de la Technologie. (Demande d'avis n° 309 970)
97-060 8 juillet 1997 (cf. Deuxième par ie p. 111)	Délibération portant recommandation relative aux annuaires en matière de télécommunications.
97-061 8 juillet 1997 (cf. Troisième partie p. 253)	Délibération portant avis sur la demande présentée par le conseil général de l'Ain concernant la prorogation de l'expérimentation du traitement automatisé relatif à la gestion de l'action sociale départementale, dénommé approche nouvelle de l'information sociale (« ANIS »).
97-062 8 juillet 1997 (cf. Troisième partie p. 224)	Délibération portant avis sur le projet d'acte réglementaire modificatif présenté par la CNAMTS concernant la prolongation de l'expérimentation du dispositif « SESAM-VITALE ». (Demande d'avis modificative n° 103 860)
97-063 8 juillet 1997 (cf. Troisième partie p. 226)	Délibération relative à une demande d'avis modificative présentée par le groupement d'intérêt public de la carte de professionnel de santé (GIP-CPS) concernant un traitement automatisé d'informations nominatives ayant pour finalité l'émission, la distribution et la gestion des cartes de professionnel de santé (CPS).
97-064 8 juillet 1997 (cf. Deuxième par ie p. 124)	Délibération portant avis sur un projet d'arrêté du ministre de l'Économie, des Finances et de l'Industrie concernant un système automatisé de gestion du renseignement sur le trafic de stupéfiants par voie maritime. (Demande d'avis n° 475 713)
97-065 9 septembre 1997	Délibération portant désignation d'un membre de la Commission nationale de l'informatique et des libertés chargé d'exercer le droit d'accès indirect en application de l'article 39 de la loi du 6 janvier 1978.

Nature-numéro date	Objet
97-066 9 septembre 1997 (cf. Première par ie p. 14)	Délibération concernant les traitements automatisés d'informations nominatives relatifs aux instruments financiers. (Norme simplifiée n° 41)
97-067 9 septembre 1997 (cf. Troisième partie p. 188)	Délibération portant avis sur un projet d'arrêté du ministère de l'Intérieur relatif aux traitements automatisés des préfectures pour l'information des personnes résidant à proximité d'une installation nucléaire sur la distribution de comprimés d'iode stable. (Demande d'avis n° 537 454)
97-068 23 septembre 1997 (cf. Troisième partie p. 219)	Délibération portant avis sur un projet de décret en Conseil d'État relatif aux transmissions d'informations d'état civil à l'INSEE en vue de la tenue du RNIPP. (Déclaration de modification n° 7916)
97-069 23 septembre 1997 (cf. Troisième partie p. 221)	Délibération relative à deux projets de décret en Conseil d'Étal concernant l'autorisation d'utilisation du répertoire national d'identification des personnes physiques par les communes dans les traitements automatisés d'état civil et par le service central d'état civil du ministère des Affaires étrangères. (Déclaration de modification n° 7916)
97-070 23 septembre 1997 (cf. Troisième partie p. 231)	Délibération concernant un projet de décret relatif aux documents conditionnant le remboursement des prestations en nature des assurances maladie, maternité et accidents du travail et contribuant à la maîtrise des dépenses de santé présenté par le ministère de l'Emploi et de la Solidarité
97-071 23 septembre 1997	Délibération décidant d'un contrôle sur place.
97-072 23 septembre 1997	Délibération décidant d'un contrôle sur place.
97-073 23 septembre 1997 (cf. Deuxième partie p. 108)	Délibération portant avis sur un traitement automatisé d'informations nominatives présenté par l'ANPE et dénommé « www.anpe.fr » ayant pour finalité une expérimentation relative à l'amélioration du rapprochement des offres et des demandes d'emplois des jeunes diplômés de la région Nord-Pas-de-Calais. (Demande d'avis n° 533 772)

Nature-numéro date	Objet
97-074 **7 octobre 1997** (cf. Troisième partie p. 152)	Délibération portant avis sur trois projets d'arrêté du maire de a ville d'Orléans concernant les différentes finalités d'une base de données foncières et fiscales. (Demandes d'avis n° 487 196, 487 202, 487 211)
97-075 **7 octobre 1997**	Délibération décidant d'un contrôle sur place.
97-076 **7 octobre 1997** (cf. Troisième partie p. 155)	Délibération portant avis sur un projet d'arrêté du maire de Clermont-Ferrand concernant l'envoi d'un courrier aux redevables de la taxe d'habitation à partir d'un fichier nformatisé transmis par l'administration fiscale. (Demande d'avis n° 524 364)
97-077 **7 octobre 1997** (cf. Troisième partie p. 277)	Délibération concernant une déclaration simplifiée du ministère de l'Économie et des Finances relative à la réalisation d'une enquête de l'INSEE sur les revenus des ménages en 1996 à partir de l'exploitation des déclarations de revenus. (Déclaration simplifiée n° 465 878)
97-078 **21 octobre 1997** (cf. Troisième partie p. 235)	Délibération relative à la demande d'avis de la Caisse primaire d'assurance maladie de Haguenau concernant l'édition de décomptes de prestations de sécurité sociale sur imprimante ibre service. (Demande d'avis n° 528 645)
97-079 **21 octobre 1997** (cf. Troisième partie p. 274)	Délibération portant avis favorable à la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête famille effectuée à la Réunion. (Demande d'avis n° 532 664)
97-080 **21 octobre 1997** (cf. Troisième partie p. 282)	Délibération portant avis sur un traitement automatisé d'informations nominatives présenté par l'ANPE dénommé « fichier historique » et ayant pour finalité l'amélioration de la connaissance des demandeurs d'emplois et de la demande d'emploi. (Demande d'avis n° 511 632)
97-081 **21 octobre 1997**	Délibération décidant d'un contrôle sur place.

Nature-numéro date	Objet
97-082 21 octobre 1997 (cf. Troisième partie p. 258)	Délibération portant avis sur la demande présentée par le conseil général des Bouches-du-Rhône et concernant la mise en oeuvre d'un traitement automatisé de données nominatives au moyen d'un dispositif de cartes à microprocesseur destiné à assurer la gestion du suivi de la prestation spécifique dépendance. (Demande d'avis n° 528 272)
97-083 21 octobre 1997	Délibération décidant d'un contrôle sur place.
97-084 4 novembre 1997 (cf. Troisième partie p. 206)	Délibération portant autorisation de mise en œuvre par le Centre de recherche en santé, travail, ergonomie de Lille d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique de la mortalité des salariés de l'usine Rhône-Poulenc d'Elbeuf. (Demande d'autorisation n° 997 040)
97-085 4 novembre 1997 (cf. Troisième partie p. 211)	Délibération portant autorisation de mise en oeuvre par le Laboratoire de santé publique de la faculté de médecine de Grenoble d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête épidémiologique sur l'asthme de l'enfant et les transports. (Demande d'autorisation n° 997 084)
97-086 4 novembre 1997	Délibération décidant d'un contrôle sur place.
97-087 4 novembre 1997	Délibération décidant d'un contrôle sur place.
97-088 18 novembre 1997 (cf. Troisième partie p. 143)	Délibération portant avis sur : — le projet d'arrêté, présenté par l'INSEE, portant création du fichier central de proposition d'inscription d'office sur les listes électorales ; — le projet de décret en Conseil d'Etat, prise en application des dispositions de l'article 18 de la loi du 6 janvier 1978 autorisant l'utilisation du répertoire national d'identification des personnes physiques pour la gestion du fichier central de proposition d'inscription d'office sur les listes électorales. (Demande d'avis n° 549 627)

Nature-numéro date	Objet
97-089 18 novembre 1997 (cf. Troisième partie p. 314)	Délibération concernant une demande d'avis portant modification du traitement d'informations nominatives « Frégate » relatif à la gestion personnalisée de la clientèle de France Télécom. (Demande d'avis no 355 807)
97-090 25 novembre 1997 (cf. Troisième partie p. 209)	Délibération portant autorisation de mise en œuvre par la direction régionale des affaires sanitaires et sociales de la région Provence-Alpes-Côte d'Azur d'un traitement automatisé d'informations nominatives ayant pour finalité une enquête d'incidence rétrospective sur six zoonoses du pourtour méditerranéen. (Demande d'autorisation n° 997 061)
97-091 25 novembre 1997 (cf. Troisième partie p. 254)	Délibération portant avis sur la demande présentée par le conseil général de l'Ain et concernant la gestion informatisée de l'aide sociale à l'enfance et de l'action sociale de terrain (ANIS-ASE). (Demande d'avis n° 532 096)
97-092 2 décembre 1997 (cf. Première par ie p. 50)	Délibération relative à un projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi n78-17 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.
97-093 2 décembre 1997 (cf. Première par ie p. 51)	Délibération 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. (Demande d'avis n° 553 059)
97-094 2 décembre 1997 (cf. Troisième partie p. 185)	Délibération relative à un projet d'arrêté présenté par le secrétariat d'état à la Santé : — d'une part, à la création par e Centre de coordination de la lutte contre les infections nosocomiales de l'inter-région Paris Nord d'un traitement automatisé d'informations nominatives ayant pour finalité de mener une enquête sur les cas d'infection à mycobactérium xénopi survenus dans la clinique du sport entre le 1er janvier 1988 et le 31 mai 1993 afin d'identifier et d'informer les patients sur un dépistage d'éventuelles lésions rachidiennes ; (Demande d'avis n° 543 691) — d'autre part, à l'utilisation du répertoire national interrégimes des bénéficiaires de 'assurance maladie à des fins de recherche des personnes perdues de vue opérées à la clinique du sport entre le 1er anvier 1988 et le 31 mai 1993.

Nature-numéro date	Objet
97-095 2 décembre 1997 (cf. Troisième partie p. 238)	Délibération relative aux vérifications sur place effectuées le 14 mai et le 11 juin 1997 auprès de la Maison des artistes.
97-096 16 décembre 1997 (cf. Troisième partie p. 294)	Délibération relative à la demande d'avis présentée par le ministère de l'Équipement, des Transports et du Logement portant création d'un traitement automatisé ayant pour finalité le contrôle des conditions de travail des conducteurs routiers (« SCAN RESO »). (Demande d'avis n° 518 712)
97-097 16 décembre 1997 (cf. Troisième partie p. 261)	Délibération portant avis sur la demande présentée par le Centre d'action sociale de la ville de Paris concernant un traitement automatisé d'informations nominatives relatif à la gestion de l'aide sociale facultative, dénommé « Paris informatisation des aides facultatives » {« PIAF »). (Demande d'avis n° 546 625)

Annexe 5

Modalités de radiation des fichiers commerciaux

Il convient de s'adresser directement aux sociétés émettrices des « mailing » que l'on reçoit ainsi qu'aux organismes de vente par correspondance dont on est client en leur demandant de ne pas céder ses nom et adresse à des entreprises extérieures. Il est aussi recommandé de s'adresser à :

- **L'Union francaise du marketing direct**

STOP PUBLICITÉ
60, rue La Boétie
75008 PARIS

Cet organisme a mis en place un système baptisé « **Stop publicité** » grâce auquel il transmet les demandes de radiation à l'ensemble de ses adhérents (vente par correspondance et presse). Il n'intervient pas auprès des sociétés non adhérentes.

- **L'Agence commerciale de France Télécom** dont on dépend.

Le service national des annuaires des télécommunications a créé la « **liste orange** » qui recense les abonnés au téléphone qui ne souhaitent pas que les informations les concernant fassent l'objet d'une cession et la « **liste SAFRAN** » qui recense les personnes ayant demandé à ne pas recevoir de prospection par télécopie ou par télex.

Les abonnés effectuant cette démarche continuent à figurer dans l'annuaire téléphonique.

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.**

Annexe 6
Vos traces sur Internet

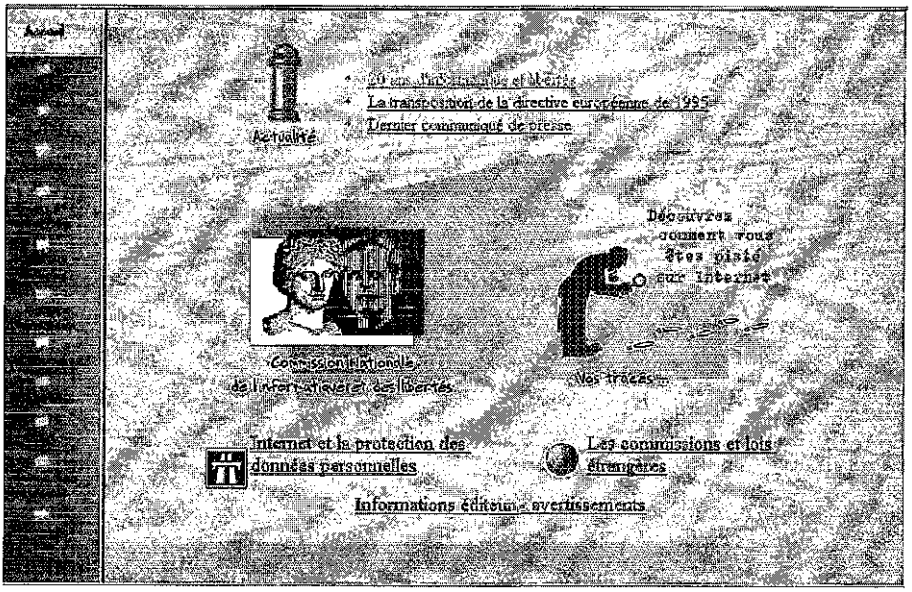


Figure 1 : Page d'accueil du site de la CNIL (http://www.cnil.fr)

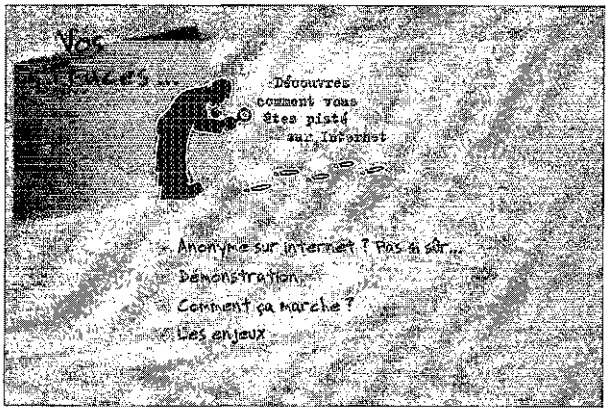


Figure 2 : Sommaire de la rubrique « Vos traces sur Internet »

Important : Le texte qui suit est la version papier de la rubrique « Vos traces sur Internet » accessible en ligne sur le site de la CNIL à l'adresse http://www.cnil.fr/traces/traces htm. Ce document est ici présenté de façon linéaire mais a été conçu à l'origine pour une lecture hypertextuelle. Les démonstrations qui figurent dans cette version reprennent une consultation effec ivement réalisée et « figée » en vue de cette publication. Les illustrations présentées dans cette rubrique sont des captures d'écrans d'un navigateur Internet.

Sommaire

ANONYME SUR INTERNET ? PAS SI SUR

Se connecter à Internet est devenu, pour la plupart des internautes, un acte quotidien. En quelques clics, la connexion est établie et vous pouvez lancer votre logiciel préféré afin d'aller visiter tel ou tel site web. Peut-être téléchargerez-vous des programmes ou des fichiers, peut-être irez-vous lire quelques messages dans les « newsgroups » sur les sujets qui vous intéressent, sans doute consulterez-vous votre messagerie. Peut-être même discuterez-vous en temps réel avec des personnes situées à l'autre bout du monde...

Que vous alliez sur Internet dans le cadre de vos activités professionnelles ou depuis votre domicile, confortablement installé dans votre fauteuil, vos déplacements dans le monde d'Internet, si vaste et si riche, vous donnent sans doute une impression de liberté. Et le fait est que vous êtes libre d'aller n'importe où sur le réseau avec le sentiment de naviguer dans un parfait anonymat. L'absence d'intermédiaire visible peut renforcer ce sentiment d'absence de surveillance. La méconnaissance du fonctionnement des réseaux peut se trouver à l'origine de cette conviction — fausse — que les connexions ne laissent pas de traces. Le préjugé très répandu qu'Internet est complexe peut donner l'assurance, hâtive, que si traces il y a, les moyens de les exploiter sont disproportionnés au regard de l'intérêt qu'on aurait à le faire.

La réalité est autre.

Non, l'anonymat n'est pas la règle sur Internet et l'absence de traces l'est encore moins. Oui, il est possible d'être sinon espionné, du moins surveillé, peut-être pas étroitement, mais suffisamment pour qu'un marché des outils de surveillance existe et que cette surveillance puisse être le fait d'acteurs de nature très diverses...

Attention, il ne s'agit pas d'affirmer que si l'anonymat n'est pas la règle, la surveillance le serait. Restons dans la réalité. Et si nous cessions un instant de qualifier Internet de « virtuel » et autre « cyber », pour le considérer sous son angle bien réel, informatique et technique, nous constaterions qu'en matière d'anonymat, Internet fonctionne exactement comme tout autre lieu du monde : l'anonymat demande des efforts, il est rarement absolu et garanti. La surveillance nécessite également des moyens, parfois importants ; elle n'est pas inéluctable, mais elle est toujours possible.

Sur cette question aux contours plutôt flous pour la plupart des personnes, le meilleur moyen d'être clair consiste à montrer directement aux personnes connectées au site de la CNIL ce qu'il est possible de collecter comme traces de leur passage.

Mieux, nous avons souhaité expliquer de la façon la plus simple possible comment nous avons procédé techniquement, en soulignant les difficultés de l'exercice, et les enjeux des techniques utilisées.

Ce que le site de la CNIL permet de faire, avec des moyens techniques limités, peut être fait par tous les sites auxquels vous vous connectez habituellement.

Cette démonstration constitue une manière de dévoilement de ce qui peut être fait, le plus souvent à votre insu.

La partie « Démonstration » exploite cinq techniques élémentaires qui permettent d'obtenir des informations sur les internautes. Jugez-vous mêmes ! Certaines techniques

peuvent ne pas fonctionner dans votre cas, selon l'ordinateur, le système d'exploitation, le navigateur ou encore la configuration réseau que vous utilisez pour vous connecter. Dans ce cas, nous vous indiquerons quelques-unes des causes qui peuvent être à l'origine d'une démonstration peu probante.

La rubrique « Comment ça marche ? » vous apprendra comment nous avons procédé. Vous découvrirez qu'aucune des techniques mises en oeuvre dans la démonstration n'est particulièrement lourde ni ne nécessite d'investissements colossaux. Bien au contraire.

« Les enjeux » :

- constater qu'aucune de ces techniques n'a été conçue à l'origine pour nuire aux internautes ou porter atteinte à leur vie privée mais qu'elles ont chacune leur justification et leur utilité ;
- indiquer que chaque technique employée a ses limites ;
- évoquer éventuellement d'autres modalités de traçage qui peuvent également être utilisées sur Internet ;
- rappeler l'attitude qu'il paraît important d'adopter lorsque l'on fait d'Internet un outil de travail, de divertissement ou d'information quotidien.

L'expérience montre que l'on est beaucoup plus conscient d'un risque si l'on en comprend les ressorts, s'il nous a été non seulement affirmé mais également expliqué.

Sur les « autoroutes de l'information », l'enjeu, c'est la protection de votre vie privée. La solution, c'est de connaître les risques et d'agir en conséquence. En un mot, d'être vigilant. Sur Internet comme ailleurs.

Nous espérons que ce site vous y aidera.

DÉMONSTRATION

Votre configuration

Démonstration

Voir figure 3 ci-contre

Pourquoi ça n'a pas marché ?

Vous utilisez peut-être un navigateur ou une version d'un navigateur soit trop ancienne soit trop récente pour figurer dans la table de comparaison qui nous permet d'analyser sa signature. Nous tentons de mettre à jour cette table régulièrement, mais il peut toujours y avoir un temps mort entre la sortie d'un nouveau logiciel et notre mise à jour. Il peut également exister des navigateurs trop exotiques que nous ne prenons pas en compte pour cette démonstration.

Par ailleurs, si Javascript n'est pas géré ou pas activé sur votre navigateur, les démonstrations qui exploitent ce langage ne fonctionneront pas.

Enfin, si votre adresse IP et votre DNS sont différents de ceux que la démonstration a indiqué, c'est peut-être parce que les informations transitent par un « firewall » ou un serveur proxy. Un « firewall » est un dispositif de sécurité situé, par exemple, au point d'entrée d'un réseau local. Il a pour effet de substituer une autre adresse IP et un autre DNS au vôtre rendant ainsi plus difficile l'identification de l'ordinateur connecté à Internet. Ce type de configuration est relativement courant dans les grandes structures (universités, grandes entreprises, etc.). On la trouve le plus souvent dès lors qu'un réseau local, plutôt qu'un PC isolé, est connecté à Internet. Quant au proxy, nous l'abordons plus en détail dans les explications relatives à la démonstration « Votre parcours sur ce site ». L'utilisation d'un proxy a pour effet de ne laisser comme adresse IP et DNS au serveur que celle du proxy.

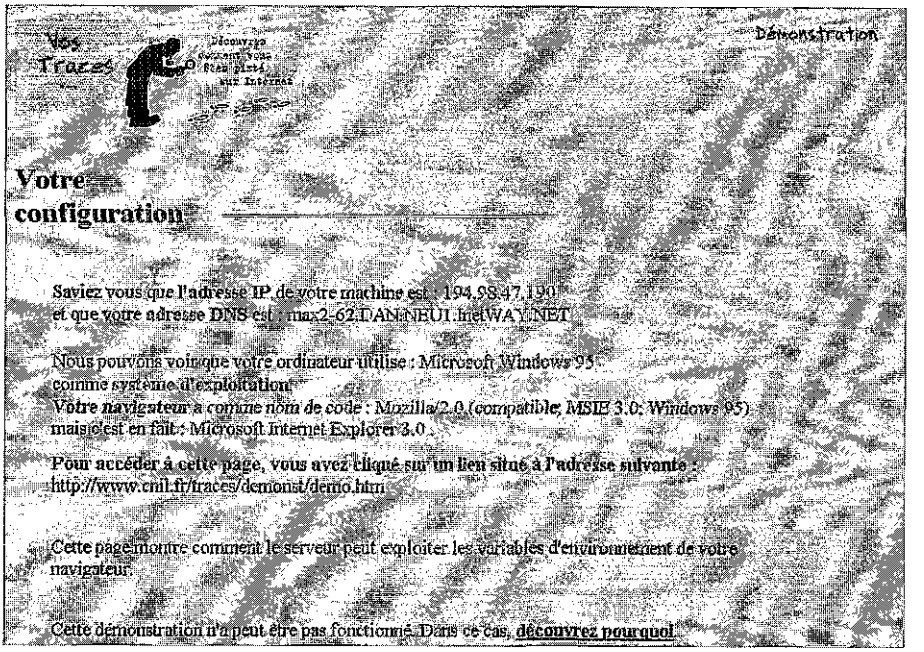


Figure 3 : Cette page vous montre que, grâce aux variables d'environnement envoyées par votre navigateur, le serveur peut savoir systématiquement quelle est votre adresse IP (194.98.47.190), votre nom de domaine (max2-62. DAN.NEU1 .InetWAY.NET) qui révèle le nom de votre fournisseur d'accès, votre système d'exploitation (Microsoft Windows 95), votre navigateur, et quelle page vous a conduit sur la page courante.

Comment ça marche ?

Pour obtenir des informations sur votre configuration et l'URL précédemment visitée, nous avons utilisé les variables d'environnement qui sont définies dans votre navigateur et que ce dernier envoie systématiquement au serveur.

Quelques explications simples...

a) Comparaison n'est pas raison
b) HTTP, Javascrpit et cie

Plus techniquement

c) Adresse IP, adresse DNS et signature du navigateur
d) lien précedemment suivi

a) Comparaison n'est pas raison

Si l'on tentait de schématiser l'ensemble des règles et procédures à suivre pour établir une communication téléphonique, on pourrait aisément distinguer deux niveaux de ce qu'il convient d'appeler des protocoles. Le premier niveau, le plus bas, est indispensable à l'établissement physique de la communication, c'est le niveau le plus technique qui permet, entre autres, de composer le numéro d'un correspondant, de générer une sonnerie sur son poste, d'établir la communication, de maintenir le transfert de la voix dans les deux sens et en même temps au travers de la ligne et enfin de terminer la communication. Le second niveau, supérieur au précédent car plus accessible aux locuteurs, n'est pas indispensable à la communication technique proprement dite mais à

la communication humaine: il part d'un accord sur la langue utilisée par les deux locuteurs en passant par les conventionnels « Allô ? », « Qui est à l'appareil ? », etc.

Sur Internet, on pourrait faire la même observation. Pour que les informations soient correctement transférées de votre ordinateur au serveur, un protocole est nécessaire afin que les différents appareils situés entre vous et lui soient à même de les transporter. Il s'agit du protocole TCP/IP. On représente généralement l'architecture d'un protocole en couches. Tout en bas, la couche matérielle correspond (schématiquement) aux câbles et aux cartes utilisés (ethemet par exemple), puis la couche réseau gère la circulation des paquets à travers le réseau (IP), la couche transport gère le flux de données entre deux machines (TCP), enfin, la couche supérieure, la couche applicative, gère les détails de communication d'une application particulière entre le serveur et le client (HTTP, par exemple, si vous êtes « sur le web », ou bien FTP, pour le transfert de fichiers, ou encore NNTP pour les « newsgroups »). La couche supérieure correspond au dialogue établit entre les deux applications client/serveur, comme par exemple votre navigateur et le serveur web.

b) HTTP, Javascript et cie

Au niveau HTTP, donc, chacune de vos requêtes contient un certain nombre d'informations, à commencer par ce que vous avez à demander : l'adresse d'une page web généralement. Mais elle contient également de nombreuses informations sur l'environnement de votre ordinateur. Ces informations sont systématiquement transmises dans chaque paquet qui part de votre ordinateur vers le serveur. Lorsque le paquet arrive sur le serveur, un processus système est créé sur la machine, processus qui intègre ces informations sous forme de variables d'environnement et exécute la requête demandée.

Autant d'informations que le serveur peut ajouter à celles dont il pourrait disposer également par ailleurs.

Concrètement, voici les variables d'environnement et leur contenu tel que nous l'avons reçu de votre navigateur : REMOTE HOST = sat23.isdn.iway.fr REMOTE ADDR= 194.98.47.202 HTTP_USER_AGENT = Mozilla/4.02 [en] (Win95; I) HTTP_REFERER = http://www.cnil.fr/traces/demonst/demo.htm

Un script sur le serveur les a analysées pour vous les présenter plus clairement : Votre adresse DNS : sat23.isdn.iway.fr Votre adresse IP : 194.98.47.202 Votre système d'exploitation : Microsoft Windows 95 Votre navigateur : Netscape Communicator 4.02 anglais Votre page précédente : http://www.cnil.fr/traces/demonst/demo.htm

c) Adresse IP, adresse DNS et signature du navigateur

Un script CGI analyse les variables d'environnement suivantes : REMOTE_HOST, REMOTE_ADDR et HTTP_USER_AGENT

REMOTE_HOST et REMOTE_ADDR retournent au serveur l'adresse DNS et l'adresse IP de votre machine. Si l'adresse DNS n'y figure pas, c'est que votre machine n'a pas été enregistrée dans le serveur de DNS.

HTTP USER AGENT est la signature du navigateur client. À partir de celle-ci, nous déterminons quel est le système d'exploitation, quelles sont les caractéristiques du navigateur (marque, modèle et, éventuellement, numéro de version) et la version linguistique du navigateur. Pour obtenir ces informations, nous utilisons une table de correspondance entre les éléments de la signature du navigateur et les signatures connues (par exemple, nous savons que la chaîne de caractère « WinNT » est contenue dans la

signature d'un navigateur Netscape tournant sous Microsoft Windows NT ou que « Windows 95 » est contenue dans la signature d'un navigateur Internet Explorer tournant sous Microsoft Windows 95).

Il est également possible pour le serveur de récupérer ces variables à l'aide d'un Javascript. Javascript est un langage de script dont les instructions s'intègrent sous forme textuelle à l'intérieure des pages HTML et que le navigateur exécute lorsqu'il charge la page. Attention, ne confondez pas Javascript et applet Java.

d) Lien précédemment suivi

Un script CGI est chargé d'analyser la variable d'environnement HTTP_REFERER, et d'en extraire les informations suivantes sur la dernière page vue par le navigateur client : protocole utilisé, adresse DNS ou IP du serveur, chemin d'accès à la ressource, et ressource demandée (page, image, cgi...).

Les enjeux des variables d'environnement

a) À quoi servent les variables d'environnement ?

Les variables d'environnement sont des outils standards mis à la disposition du programmeur par les systèmes d'exploitation. Elles permettent de sérieusement faciliter la programmation. En plaçant des informations dans des variables, d'autres applications peuvent les manipuler aisément. De nombreux logiciels créent ainsi des variables d'environnement, c'est le cas de votre navigateur.

Ces informations sont transmises au serveur web pour lui permettre de prendre en compte des éléments propres à votre configuration. Connaître, par exemple, le type de navigateur que vous utilisez et sa version peut permettre au serveur de ne pas lancer certaines applications qu'il sait ne pas être compatibles avec lui.

La variable qui contient les références de la dernière page à laquelle vous avez accédé permet, par exemple, aux sites qui achètent des bandeaux publicitaires de comptabiliser le nombre de connexions qui ont été effectuées immédiatement après un clic sur une des pages comportant tel ou tel bandeau, ce qui permet d'en évaluer l'efficacité.

b) Faut-il avoir peur des variables d'environnement ?

S'il n'y avait que les variables d'environnement, il n'y aurait pas lieu de s'inquiéter étant donné leur contenu. Le problème naît de l'association de ces variables avec les autres informations que le serveur a pu glaner sur vous par ailleurs et le lien qu'il peut éventuellement faire avec les « cookies » ou les fichiers d'audit pour conserver une trace de votre configuration d'une session à l'autre.

Alors, les variables d'environnement méritent-elles que l'on en ait peur ? Ou sont-elles un exemple supplémentaire d'une peur qui serait générée par ce que l'on ne connaît pas ?

[es *limites des variables d'environnement*

Il n'y a pas beaucoup de moyens de mettre en échec les variables d'environnement.

a) Bricoler

Il est certes techniquement possible de vous plonger dans le code exécutable de votre navigateur pour aller modifier la façon dont celui-ci signe son passage.

Mais :

— cela nécessiterait de votre part une bonne connaissance de la programmation ;
— c'est rigoureusement interdit la plupart du temps par le producteur du navigateur, dans la mesure où lorsque vous utilisez le logiciel, vous vous engagez le plus souvent à ne pas le modifier ni à le décompiler, enfin ;
— vous risqueriez d'endommager sérieusement votre logiciel.

b) Utiliser soit une antiquité, soit la toute dernière version

Si vous utilisez un logiciel particulièrement ancien ou particulièrement récent, il est possible que la table de concordance que nous utilisons pour comprendre la signature de votre navigateur ne contienne pas d'entrée pour le vôtre. Dans ce cas, notre script restera muet.

c) Désactiver Javascript

Si la lecture a été faite en Javascript, il est probable qu'elle ne fonctionnera pas si Javascript n'est pas géré ou pas activé sur votre navigateur.

Un peu de météo

Démonstration

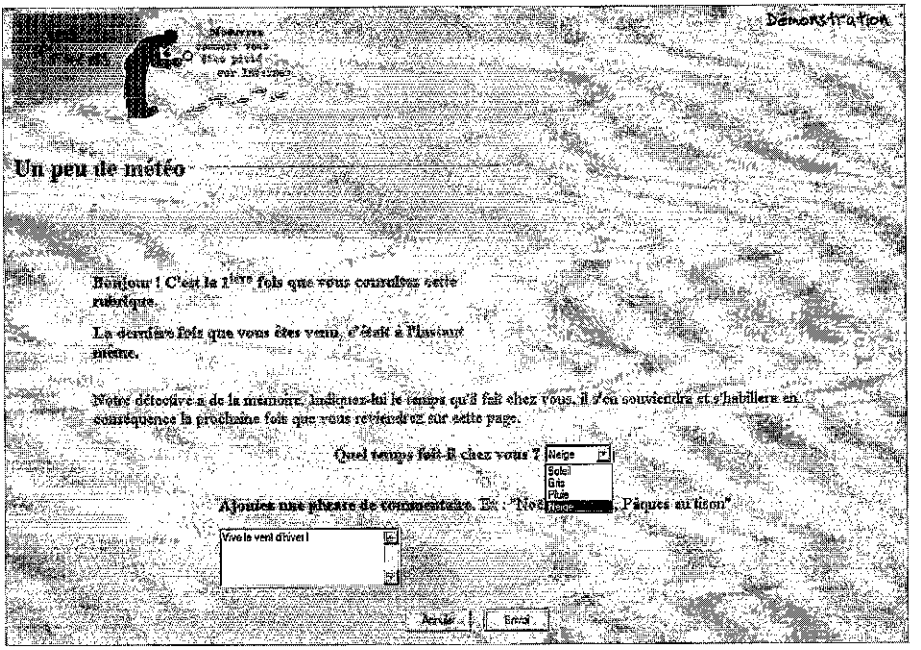


Figure 4 : Grâce aux cookies, le serveur voit que c'est la première fois que vous chargez cette page. En cliquant sur « Envoi », le climat (ici « Neige ») que vous avez sélec ionné et la phrase que vous avez tapée (« Vive le vent d hiver ») sont envoyés au serveur...

La figure 5 ci-contre montre comment un serveur peut exploiter les « cookies ».

Si cette démonstration n'a pas fonctionné, voici peut-être pourquoi.

Pourquoi ça n'a pas marché ?

Si la démonstration que nous avons mise en place n'a pas fonctionné, cela peut être pour plusieurs raisons :

- votre navigateur ne prend pas les « cookies » en compte soit parce qu'il n'a pas été prévu pour cela (c'est le cas des anciennes versions des produits de Microsoft et Netscape) soit parce que vous l'avez paramétré pour qu'il les évite. La démonstration en Javascript peut ne pas fonctionner si Javascript n'a pas été activé sur votre navigateur ;
- vous avez déplacé, modifié ou supprimé le fichier qui contient les « cookies » sur votre ordinateur et votre navigateur ne peut plus y accéder.

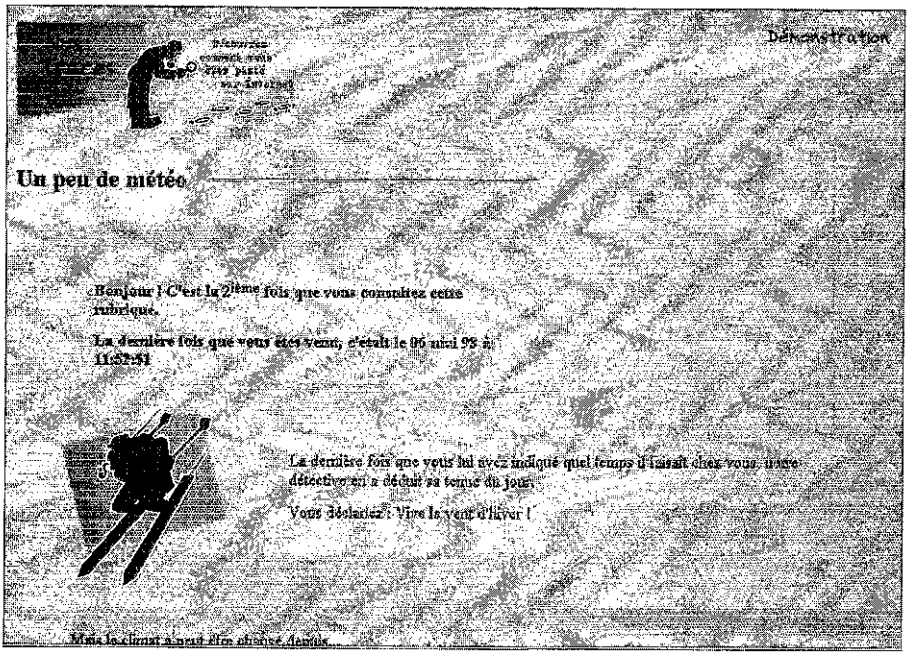


Figure 5 : ... Le serveur vous montre qu'il a bien compris les informations que vous lui avez envoyées (le détective fait du ski car vous lui avez indiqué « Neige », la phrase est bien là). Il est capable d'indiquer l'heure, la date et le numéro de la dernière visite. A chaque chargement ultérieur de la page, ces informations seront remises à jour dès lors que vous utilisez le même ordinateur elle même logiciel. Ces informations sont en fait sur vôtre disque dur dans des cookies.

Attention ! : Les « cookies » ne sont sauvegardés sur votre disque dur que lorsque vous quittez votre navigateur.

Comment ça marche ?

Pour compter vos passages, nous rappeler de la date de votre dernière visite et pratiquer la météo avec notre détective, nous avons utilisé des « cookies ».

Quelques explications simples...

a) Qu'est-ce qu'un « cookie » ?
b) Un peu plus de détails ?
c) Cookies et navigateurs

Plus techniquement...

d) L'écriture des « cookies »
e) La lecture et l'affichage des « cookies » par un CGI
f) Le répertoire qui contient les « cookies »

a) Qu'est-ce qu'un « cookie » ?

Pour aller à l'essentiel, on peut dire qu'un « cookie » est un enregistrement d'informations par le serveur dans un fichier texte situé sur l'ordinateur client (le vôtre), informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement. La technique des « cookies » repose sur le protocole HTTP, c'est-à-dire le protocole du web. Il ne faut donc pas voir de « cookies » partout : seul un serveur web peut en envoyer.

Plus précisément, un « cookie » se compose d'un ensemble de variables (ou de champs) que le client et le serveur s'échangent lors de transactions HTTP, lesquelles variables sont tout simplement stockées sur la machine cliente dans un simple fichier texte. Un « cookie » est obligatoirement rattaché à un nom de domaine et un ensemble d'URL de telle sorte que seule une requête provenant du même serveur pourra y accéder.

Par exemple, grâce à un programme CGI, le serveur a la possibilité de mettre à jour ou d'effacer un « cookie » Mais pour cela, il doit spécifier tous les attributs du « cookie » par conséquent seul le serveur qui a créé un « cookie » peut le modifier ou le supprimer.

Un même « client » peut stocker un maximum de trois cents « cookies », dont vingt maximum pour un même serveur, chaque « cookie » pouvant atteindre jusqu'à 4000 octets (env. 4 Ko).

Le paragraphe suivant donne quelques précisions sur le fonctionnement des « cookies » dont vous pouvez éventuellement vous dispenser si les détails techniques vous rebutent. Sachez simplement que leur fonctionnement est extrêmement simple : le fichier stocké sur votre PC est un fichier texte écrit et lu par votre navigateur. Vous pouvez le lire, le détruire, le copier, le modifier à la main si vous le souhaitez. Il ne peut pas contenir de virus ni être exécuté, il n'est pas actif.

b) Un peu plus de détails ?

Un « cookie » est envoyé par le serveur par insertion d'une directive dans l'en-tête du message de réponse HTTP dont la syntaxe est la suivante :

Set-Cookie : Nom=valeur; expires=date; path=chemin; domain=nom_domain; secure

Grâce à l'information « Nom=valeur », (ex : « datenaissance=01011964 ». C'est vous qui avez tapé « 01011964 » dans un formulaire) chaque « cookie » porte un nom (« datenaissance », dans notre exemple) auquel correspond une valeur définie par le serveur sous forme d'une chaîne de caractères et qui, précisément, sera renvoyée au serveur lors des connexions suivantes (« 01011964 »). Le champ « expires » indique la date d'expiration du « cookie ». Une fois cette date dépassée, le logiciel client n'insérera plus le « cookie » lors des transactions HTTP. Le serveur peut donc effacer un « cookie » en substituant à sa date initiale d'effacement une date antérieure à la date du jour. Le champ « path » indique quelles pages peuvent accéder au « cookie » à partir du serveur spécifié dans domain=nom_domain, où l'on retrouve le nom de domaine du serveur qui a posé le « cookie » (www.cnil.fr, par exemple). Par défaut, ces deux dernières valeurs correspondent à la page et au domaine qui ont initialisé le « cookie ». Enfin, « secure » est utilisé pour n'assurer l'application du « cookie » que lorsque la connexion client-serveur est sécurisée, par le protocole HTTPS par exemple. En l'absence de ce champ, le « cookie » est transmis quel que soit le protocole utilisé.

Par exemple, lors de la démonstration, vous nous avez envoyé les informations suivantes :

— temps= « Pluie » ;
— phrase= « Ceci est un commentaire ! »

Nous vous avons renvoyé les « cookies » suivants :

Set-Cookie: Temps=Pluie; expires=Monday, 06-Jun-98 09:23:25 GMT; domain= www.cnil.fr; path=/

Set-Cookie: Phrase=Ceci est un commentaire !; expires=Monday, 06-Jun-98 09:23:25 GMT; domain=www.cnil.fr; path=/

Lorsque le client accède à une URL, il recherche parmi ses « cookies » celui ou ceux qui correspondent à l'URL. Il insère ensuite dans la requête HTTP une ligne contenant

tous les couples « nom=valeur » correspondants. Les « cookies » posés par un serveur sont donc systématiquement envoyés à ce serveur sans qu'il ait besoin de les réclamer.

Un « cookie » peut être posé et lu grâce à un programme CGI exécuté sur le serveur ou par un Javascript intégré dans une page HTML (attention : ne confondez pas Javascript et applet Java).

c) « Cookies » et navigateurs

Les principaux navigateurs du marché reconnaissent les « cookies » mais les navigateurs plus anciens ou moins performants les ignorent. S'agissant des produits de Netscape et de Microsoft, leur méthode de stockage des « cookies » est légèrement différente. Là où le navigateur enregistre tous les « cookies » dans un seul fichier, l'explorateur crée un fichier « cookie » par serveur qui contient tous les « cookies » de ce serveur, lequel fichier est situé dans un répertoire « cookies » La présentation interne du fichier est également différente mais on retrouve toutes les informations et il s'agit toujours d'un simple fichier texte.

À vous de vérifier les « cookies » envoyés par la CNIL (voir *infra* f) le répertoire qui contient les « cookies »).

Attention ! : Les « cookies » ne sont sauvegardés sur votre disque dur que lorsque vous quittez votre navigateur.

d) L'écriture des « cookies »

Nous utilisons deux scripts CGI : un CGI pour collecter les informations (que l'utilisateur aurait éventuellement saisies lors d'une précédente visite), et un CGI chargé de mettre à jour les « cookies » lorsque l'utilisateur a fini de remplir le formulaire.

- Collecte des informations : le premier script se charge de la collecte de deux « cookies » (« Temps » et « Phrase ») et affiche leurs valeurs dans la page.

- Mise à jour du « cookie » : le deuxième script CGI effectue les opérations suivantes : il récupère les informations saisies par l'utilisateur grâce au formulaire, puis insère dans l'en-tête d'un message HTTP les « cookies » suivants :

Set-Cookie: Temps=Pluie; expires=Monday, 06-Jun-98 09:23:25 GMT; domain= www.cnil.fr; path=/

Set-Cookie: Phrase=Ceci est un commentaire !; expires=Monday, 06-Jun-98 09:23:25 GMT; domain=www.cnil.fr; path=/

Le contenu du message HTTP renvoyé est un indicateur de retour sur cette page.

e) La lecture et l'affichage des « cookies » par un CGI

Bonjour ! C'est la deuxième fois que vous consultez cette rubrique.

La dernière fois que vous êtes venu, c'était le 06 avril 98 à 09 : 23 : 00

Nous utilisons deux scripts CGI : un premier script est chargé de collecter les « cookies » concernant le nombre de visites et la date de dernière visite. Un second CGI va se charger de mettre à jour les « cookies ».

1) Collecte des « cookies » : le script CGI récupère les « cookies » que lui envoie le navigateur client, puis extrait de ces derniers ceux qui correspondent aux nombres de visites de l'utilisateur, et la date de dernière visite. La dernière opération consiste à afficher :

- la valeur du « cookie » +1 (la visite en cours) ;
- la valeur du « cookie » contenant la date de dernière visite.

2) Mise à jour du « cookie » : le deuxième script CGI effectue les opérations suivantes :

— il formate la date courante pour le « cookie » Derniere visite=d et collecte, analyse et incrémente le « cookie » Nombre visite=n ;

- Ensuite, il renvoie au client les nouvelles valeurs des « cookies » sous la forme Nombre_vi-site=n et Dernière_visite=d dans l'en-tête du message HTTP. Le contenu du message HTTP renvoyé est une image d'un pixel transparent (donc invisible par l'utilisateur).

f) Le répertoire qui contient les « cookies »

La sauvegarde des « cookies » est organisée différemment selon le type de navigateur que vous utilisez. Si nous considérons les deux principaux navigateurs existants :

- Microsoft Internet Explorer gère un répertoire « cookies » dans lequel se trouvent des fichiers au format texte. Les « cookies » sont enregistrés dans des fichiers ayant comme nom le DNS du site qui vous les a envoyés.

L'emplacement du répertoire « cookies » dépend de votre système d'exploitation.

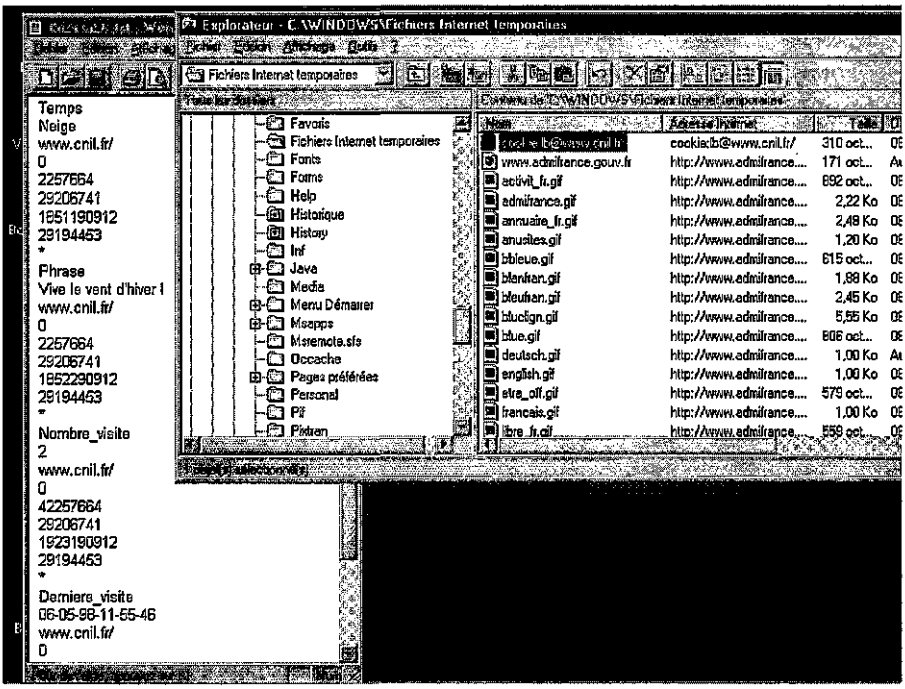


Figure 6 : Avec Microsoft Internet Explorer 3 0, les fichiers cookies sont rassemblés par site d'origine (ici la CNIL) dans un répertoire « Fichiers Internet temporaires » sous le répertoire « Windows » (fenêtre de droite). A gauche, le fichier cookies de la CNIL est ouvert. On y retrouve les informations saisies dans la page « Un peu de météo » (« Temps=neige », « Phrase=Vive le vent d'hiver 1 »).

Système d'exploitation	Répertoire
Windows 95	C:\Windows\Cookies\
Windows NT	C:\WinNt\Cookies\
Unix	*/home/* .microsoft/Cookies *home :* Chemin d'accès à votre répertoire personnel.
Macintosh	*folder:*Préférences Panel:Cookies *folder :* Dossier dans lequel est installé votre navigateur.

- **Netscape Navigator/Communicator** enregistre les « cookies » au sein d'un seul fichier : « cookies txt ».

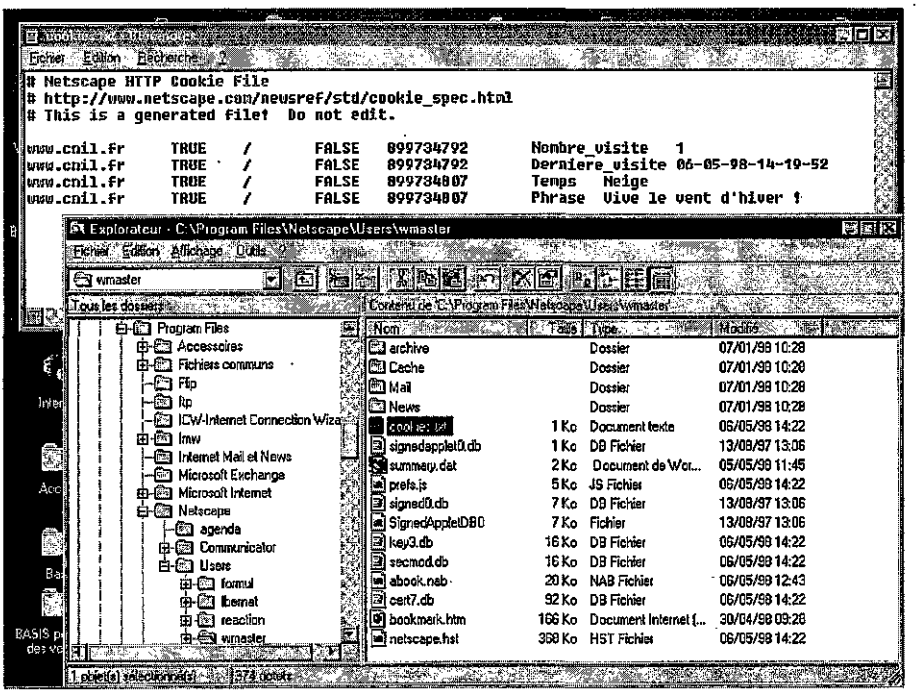


Figure 7 : Avec Netscape Navigator 4.0, un seul fichier « cookies. txt » rassemble tous les « cookies » envoyés au navigateur.

Ce fichier au format texte contient l'ensemble des « cookies », quel que soit le site qui vous les a envoyés. L'emplacement de ce répertoire dépend du répertoire dans lequel vous avez installé votre navigateur.

Navigateur	Système d'exploitation	Répertoire
Navigator	Windows 95	C:\Program Files\Netscape\Navigator\Cookies.txt
Navigator	Windows NT	C:\Program Files\Netscape\Navigator\Users\name\ Cookies.txt *name :* "Default" ou nom d'utilisateur sous lequel vous vous connectez.
Communicator	Windows 95 Windows NT	C:\Program Files\Netscape\Communicator\Users\ name\Cookies.txt *name :* "Default" ou nom d'utilisateur sous lequel vous vous connectez.
Navigator Communicator	Unix	*ıome/,* netscape/cookies terne : Chemin d'accès à votre répertoire personnel.
Navigator Communicator	Macintosh	*folder.* MagicCookie *folder :* Dossier dans lequel est installé votre navigateur.

Les *enjeux des « cookies »*

a) À quoi servent les « cookies » ?

Les « cookies » peuvent être utilisés à des fins très diverses. L'utilisation qui en est faite ici dans un souci de pédagogie constitue un exemple parmi d'autres. Prenons un cas concret de ce que nous aurions pu faire, mais que nous ne faisons évidemment pas : dans la rubrique de ce site intitulée « Comment déclarer vos traitements ? », vous avez la possibilité de commander des formulaires de déclaration à la CNIL en nous laissant vos coordonnées. Nous aurions pu à cette occasion déposer dans votre ordinateur un « cookie » contenant ces coordonnées. Libre à nous, ensuite, de faire le lien entre votre adresse IP et votre adresse postale afin de prendre connaissance de manière nominative du parcours que vous avez suivi. Tiens, vous avez consulté tel dossier thématique ! Tiens, vous avez consulté tel communiqué de presse... Nous aurions pu ainsi, à votre insu, constituer un premier profil de votre comportement, associé à vos coordonnées !

Bien sûr, rien de tout cela n'a été mis en place sur ce site dont le maître mot est la transparence, cette rubrique en est la preuve. Mais d'autres sites sont moins transparents que celui-ci.

Voici quelques exemples d'autres utilisations possibles :

- un serveur d'actualité ou d'articles de presse vous demande de remplir un formulaire pour indiquer vos préférences (sports : football, politique : écologie, spectacle : cinéma), afin de les stocker dans un « cookie » sur votre PC pour vous présenter directement, lors de vos prochaines connexions, les informations correspondant à ces préférences ;
- un serveur de commerce électronique insère un « cookie » à chaque fois que l'utilisateur sélectionne un produit, au même rythme que celui du remplissage d'un caddie. Lorsque l'utilisateur se rendra sur la page contenant le formulaire de commande, le serveur récupérera l'ensemble des « cookie » du « caddie » afin d'afficher l'ensemble des produits sélectionnés par le client ;
- un moteur de recherche de site positionne des « cookies » en fonction des rubriques visitées par le client (ex. : informatique, musique, santé) afin, ultérieurement, d'afficher dynamiquement des bandeaux publicitaires correspondant aux goûts ainsi décelés ;
- un serveur propose à l'utilisateur de choisir lui-même la couleur du fond d'écran, la présence de multi-fenêtrage ou encore les polices de caractère utilisées. Il stocke toutes ces informations dans des « cookies » et présente au client une page d'accueil correspon dant précisément à ses goûts graphiques.

Ces différentes situations montrent le grand avantage des « cookies » : ils dispensent d'un stockage sur le serveur. Leur inconvénient principal est que si l'internaute utilise une machine différente, les « cookies » de sa machine habituelle seront introuvables. De plus, le serveur ne peut jamais être sûr que le fichier texte qui contient le « cookie » n'aura pas été effacé ou modifié directement par l'internaute. C'est pourquoi les « cookies » sont souvent exploités pour une seule utilisation au cours d'une même session.

Les informations figurant dans le « cookie » peuvent être claires ou codées. C'est le serveur qui décide. Cela peut, par exemple, être un code qui renvoie à des informations stockées sur le site. Si, par exemple, vous remplissez des formulaires, le serveur peut les enregistrer sur son disque sous un numéro et stocker ce numéro dans un « cookie » sur votre PC. Ce qui lui évite de vous demander votre identité tout en lui permettant ultérieurement de faire le lien avec vous lors d'une prochaine session.

En particulier, et sans avoir besoin d'utiliser les fichiers d'audit du serveur, les « cookies » peuvent permettre à un serveur de déterminer votre parcours durant une session et de vous « profiler » en conséquence. Il suffit au serveur de positionner un « cookie » à chaque page ou lors de chaque action que vous faites puis de les récupérer globalement afin d'analyser votre chemin. Rien n'empêche alors de vous proposer des

pages créées dynamiquement en fonction de votre profil ! Les serveurs qui utilisent de nombreux « cookies » le font souvent à cette fin.

Mais comment distinguer le serveur qui utilise les « cookies » pour améliorer, en quelque sorte, le confort de votre consultation et ceux qui vous traquent et vous pistent à votre insu en utilisant le même moyen ?

b) Faut-il avoir peur des « cookies » ?

Un serveur ne peut pas disposer par le biais des « cookies » d'informations que vous n'auriez pas précédemment diffusées. Par conséquent, les « cookies » ne pourraient lui dévoiler votre nom que si vous l'aviez donné précédemment dans un formulaire. En outre, seul le serveur à qui vous avez donné cette information pourrait l'exploiter plus tard.

Le problème des « cookies » est lié à leur obscurité, leur contenu étant rarement explicite : suite de chiffres, de lettres, codes, clés... Au-delà de l'impression de manipulation que cette technique peut produire, et même en sachant qu'un « cookie » ne peut pas contenir grand chose ni avoir d'action particulière, on reste étonné qu'un serveur distant puisse placer des informations sur l'ordinateur d'un internaute sans avoir particulièrement à s'expliquer sur son contenu, l'utilisation qu'il en fera, etc.

Si vous utilisez particulièrement un serveur très interactif, il y a des chances qu'un jour ou l'autre, vous lui envoyiez un mail à partir d'une page web, ou que vous répondiez à une demande un peu plus nominative de sa part. Ce jour-là, n'oubliez pas que tous les « cookies » positionnés auparavant et auxquels vous n'avez pas prêté attention pourront être mis en relation avec l'information beaucoup plus précise que vous lui transmettez.

Enfin, si vous effectuez votre session à partir d'un ordinateur qui n'est pas le vôtre ou si votre ordinateur est utilisé par un tiers, sachez que chaque « cookie » posé par un serveur est une trace qui reste sur le disque dur et indique le passage sur ce serveur. Et vous n'avez pas nécessairement envie que cette visite soit connue de l'utilisateur suivant.

Alors, faut-il avoir peur des « cookies » ? Évidemment non ! Il faut toutefois savoir comment s'en préserver lorsqu'ils ne semblent pas utiles et exiger des sites qui les exploitent plus de transparence et d'engagement de leur part, conformément aux principes de protection des données personnelles reconnues par les législations européennes et tout particulièrement en France par la loi du 6 janvier 1978.

[es *limites des* « *cookies* »

a) Radicalement

Pour être absolument sûr de ne pas traîner de « cookies » indésirables, la méthode la plus radicale consiste à utiliser des navigateurs incapables de les traiter. C'est le cas des plus anciens et de certains autres qui ont volontairement choisi de ne pas exploiter cette fonctionnalité. Mais ce choix conduit également à vous couper des autres évolutions de ces navigateurs.

b) À la carte

Les navigateurs de dernière génération proposent dans leurs options de paramétrage de contrôler les « cookies » en direct, au moment où ils arrivent. Concrètement, lorsque le « cookie » vous est envoyé par le serveur, une fenêtre s'ouvre et indique « le serveur www.cnil.fr vous a envoyé un « cookie » dont le contenu est « xxxx » souhaitez-vous le conserver ? ». Si vous répondez par la négative, le « cookie » n'est pas enregistré, votre navigateur ne le prend pas en compte. Cette solution présente un avantage et un inconvénient : d'un côté, l'on prend enfin en compte l'avis de l'internaute, de l'autre, la multiplication de l'annonce des « cookies » parasite en permanence son écran à tel point qu'il finit par passer plus de temps à accepter ou refuser des « cookies » qu'à consulter le site.

c) Radicalement bis

C'est pourquoi il est également possible dans les derniers navigateurs (Microsoft et Netscape en particulier) de refuser une fois pour toutes les « cookies ». Mais attention : qui refuse les « cookies » systématiquement se prive peut-être de « cookies » qui lui simplifieraient la vie, voire même s'interdit l'utilisation de certains sites dont le fonctionnement interactif repose sur eux...

d) Manuellement

L'autre option consiste à accepter tous les « cookies » et à aller nettoyer périodiquement les fichiers qui les contiennent. Il suffit d'ouvrir le fichier « cookie » avec un éditeur de texte standard, de le modifier et de l'enregistrer. Il peut aussi être supprimé purement et simplement.

Cette démarche est particulièrement constructive car elle permet à chacun de voir très clairement quels serveurs les utilisent, ceux dont les « cookies » ont un contenu incompréhensible, ceux qui sont plus clairs, etc. Il est vrai qu'à la longue, cette exploration peut être lassante.

Votre parcours sur ce site

Démonstration

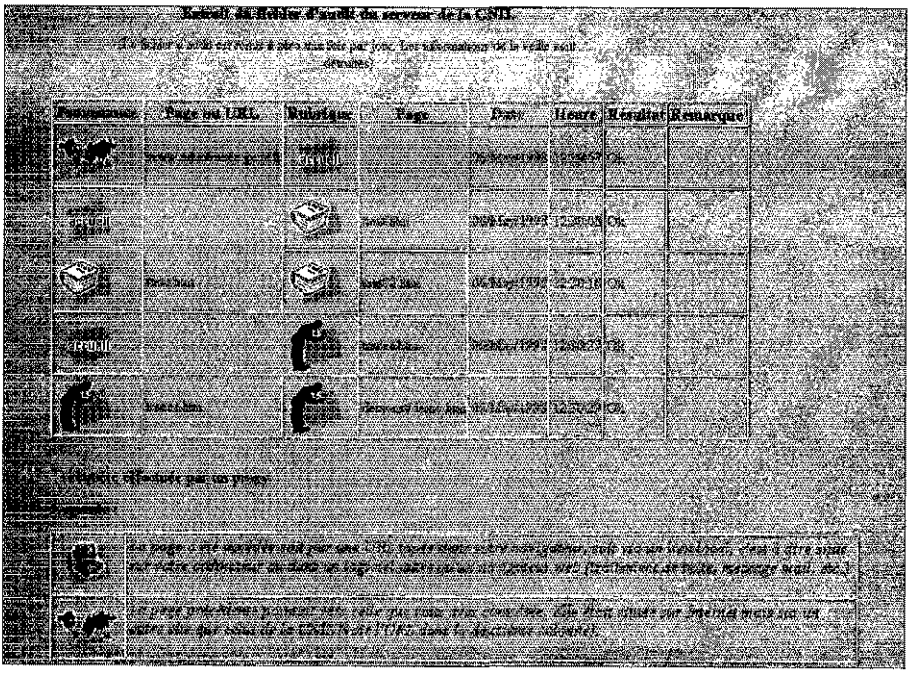


Figure 8 : En analysant le fichier d'audit, le serveur peut se rappeler votre parcours sur le site : vous êtes arrivé en cliquant sur un lien situé sur www.admifrance.gouv.fr vers le site de la CNIL (page d'accueil), puis vous avez été sur le sommaire de la rubrique « Textes », vous avez chargé la loi Informatique et libertés (text02.htm), un clic sur la barre de gauche, considérée comme un élément statique de la page d'accueil, vous a conduit sur le sommaire de la rubrique « Vos traces... » (traces.htm) puis sur le sommaire des démonstra ions (demonst/demo htm) avant d'arriver sur la page du parcours (non affichée dans le tableau).

La figure 8 ci-dessus présente plus agréablement les informations figurant dans le fichier d'audit du serveur. Pour vous donner une idée plus précise de sa forme réelle, voici les informations disponibles dans notre fichier d'audit sur votre dernière page consultée : sat31.isdn.iway. fr - - [06/Apr/1998:09:29:26+0000]"GET/traces/demonsî/demo. htm HTTP/1.0" 200 2355 "http://www.cnil.fr/traces/traces.htm" "Mozilla/4.02[en] (Win95;I)"

Cette page montre comment le serveur peut exploiter son fichier d'audit pour vous suivre.

Si cette démonstration n'a pas fonctionné, voici peut-être pourquoi.

Pourquoi ça n'a pas marché ?

Si vous avez constaté que les informations que le serveur vous a retournées sont erronées, cela peut avoir plusieurs causes. En toute logique, cela signifie que l'adresse IP que nous avons reçue lors de vos différentes requêtes n'était pas la vôtre ou pas seulement la vôtre. Ceci peut se produire, par exemple, dans les cas suivants :

a) Le cybercafé : la cabine téléphonique du net

Si vous vous êtes connecté en utilisant un ordinateur en libre service, comme par exemple dans un cybercafé, ou à partir d'une borne située dans un lieu public, un internaute a peut-être visité notre site avant vous à partir du même ordinateur et a donc laissé la même trace que vous, trace que nous vous avons présentée. Notre fichier d'audit est remis à zéro toutes les 24 heures, par conséquent, si plusieurs personnes se sont connectées dans la journée, toutes leurs connexions apparaissent également. Cette situation peut être assimilée à celle d'une cabine téléphonique.

b) Le « firewall », ou comment avoir une adresse IP « de paille »

Si vous vous êtes connecté à travers un réseau local, il est possible qu'un « firewall » soit en place et cache votre véritable adresse IP en la remplaçant par une autre. Plus précisément, le « firewall » situé à la sortie du réseau local de votre entreprise substitue une autre adresse IP à la vôtre et se charge lui-même de la distribution des paquets à leurs bons destinataires. C'est une sorte d'intermédiaire qui anonymise votre session, à la façon d'un homme de paille. Il peut ainsi utiliser une même adresse IP pour plusieurs personnes et réorganiser lui-même la distribution des paquets aux bons destinataires sur le réseau local. La trace laissée dans le fichier d'audit du serveur est donc celle du « firewall » et non la vôtre. Un tel dispositif est généralement installé pour des raisons de sécurité, afin d'éviter toute intrusion extérieure sur le réseau local et d'anonymiser les requêtes des ordinateurs du réseau.

Ce qu'il importe de savoir, lorsqu'un tel dispositif est mis en place, c'est que tout ce qu'un serveur peut faire en terme de traçage d'adresse IP et de fichier d'audit, un « firewall » peut le faire encore mieux ! Ainsi, ce n'est plus le serveur Internet qui peut vous suivre à la trace mais l'administrateur du « firewall » probablement situé dans votre entreprise. Et dans ce cas, il ne disposera pas seulement de votre parcours sur un serveur particulier, il disposera de toutes vos requêtes et sera en mesure de reconstituer entièrement vos sessions puisque toutes vos requêtes transiteront nécessairement par le « firewall », point d'accès unique de votre réseau local à Internet.

Si votre entreprise utilise un « firewall », les informations que nous avons retournées ne sont peut-être pas les vôtres.

c) Le serveur de proxy : cache-cache

Un serveur proxy peut être situé sur tout point du réseau mais l'est généralement chez votre fournisseur d'accès. Lorsque vous exécutez une requête vers un serveur du réseau, le proxy en question vérifie si la même requête a déjà été faite précédemment.

Si c'est ce n'est pas le cas, il la lance pour vous, et vous transmet son résultat — par exemple la page HTML demandée — après l'avoir enregistré sur son disque dur. Ainsi, si vous ou un autre client du fournisseur d'accès lance la même requête peu de temps après, c'est le serveur de proxy qui y répondra en allant la chercher simplement sur son disque dur. D'où un gain considérable en temps et une économie de bande passante pour le fournisseur d'accès. Votre page écran se chargera beaucoup plus vite. Schématique-ment, c'est exactement le principe de la mémoire cache que l'on trouve sur les disques durs et dans les microprocesseurs.

Cette situation implique deux conséquences :

- c'est la trace du proxy qui figurera dans le fichier d'audit du serveur Internet que vous avez contacté ;
- le proxy, lui, pourra très bien conserver l'intégralité de l'historique de toutes vos requêtes. Si le proxy est situé dans votre entreprise, la configuration est la même que dans le cas du « firewall » ci-dessus : l'administrateur du proxy peut reconstituer toutes vos transactions. S'il est chez votre fournisseur d'accès, c'est ce dernier qui dispose de ces informations.

Imaginons qu'un internaute se livre à des opérations qui portent atteinte à des personnes (diffamation, injure, propos racistes, etc.). Le serveur auquel se plaindrait la victime ou par lequel transiteraient les paquets qui causent des dommages à autrui, pourrait très bien informer votre fournisseur d'accès — dénoncer une infraction est une obligation légale — qui pourrait alors vous sanctionner en annulant votre abonnement. La victime pourrait aussi taire appel à la justice et c'est un magistrat qui rapprocherait le journal des connexions du fournisseur d'accès et le fichier d'audit du serveur sur lequel les malversations auraient eu lieu.

Quoi qu'il en soit, si votre fournisseur d'accès utilise un proxy, il y a des chances pour que les informations que nous vous avons renvoyées soient inexactes.

d) Des anonymiseurs professionnels

Dernier cas de figure : certains sites vous proposent de jouer le rôle d'anonymi-seur. Concrètement, vous vous connectez sur un site web anonymiseur A. Il vous propose de taper l'adresse d'un autre serveur B à l'intérieur d'une page web dans une boîte de saisie. Puis le serveur A envoie la requête vers B, lequel transmet à A le résultat de sa requête. A re-dirige alors sur vous ce résultat. Le fichier d'audit de B confient donc l'adresse IP de A, et seul Te fichier d'audit de A contient votre adresse IP. Pour vous identifier, l'administrateur du serveur B devrait demander au serveur A un extrait de son fichier d'audit, ce que A, a *priori,* refuserait de faire (c'est du moins ce que ce type de serveurs annoncent). Il faut noter tout de même que si lui, l'anonymiseur, vous a tracé, il est en mesure de savoir à quoi vous vous intéressez et, mieux encore, il sait que vous souhaitez rester anonyme.

Si vous avez utilisé un anonymiseur, théoriquement, nous n'avons pas été en mesure de vous tracer correctement, si l'on ose dire ! '

Comment ça marche ?

Pour suivre votre parcours sur notre site, nous avons extrait du fichier d'audit de notre serveur les informations correspondant à votre adresse IP.

a) Un client, un serveur, des requêtes
b) Des adresses IP
c) Des paquets
d) Un paquet pour le 22 à Asnières
e) Comment voir les paquets
f) Un peu d'imagination
g) Plus techniquement...

a) Un client, un serveur, des requêtes

Lorsque vous cliquez sur un lien sur la page d'un site web, le logiciel que vous utilisez sur votre ordinateur envoie au serveur qui héberge cette page un message du type « envoie-moi la page située à l'adresse « xxx.xxx.xx/yyyy/zz.html ».

Cette page n'est rien d'autre qu'un fichier (« zz.html ») situé sur un répertoire de l'ordinateur serveur.

On parle donc de client, de serveur et de requêtes.

Tout comme dans un restaurant, le client formule des requêtes à un serveur lequel lui répond en lui envoyant (servant) un résultat. Soit le résultat correspond à la requête formulée, soit le client reçoit un message d'erreur du type « le serveur n'a pas trouvé la page demandée ». Ceci est extrêmement schématique mais constitue le fonctionnement de case de toute transaction sur Internet. Vous êtes le client, le serveur est le site de votre choix et vos requêtes correspondent aux actions que vous faites sur votre navigateur pour passer d'un lien à l'autre (soit en cliquant sur des liens, soit en tapant directement les adresses).

b) Des adresses IP

Or, pour que le serveur puisse vous envoyer le résultat de votre requête, à vous et uniquement à vous, il faut qu'il ait votre adresse. Vous, vous avez la sienne, mais lui, tant que vous ne lui envoyez pas de requête, n'a pas la vôtre. Lorsque votre ordinateur envoie sur le réseau votre requête, il la compose d'une façon normalisée, en respectant un protocole. Sur Internet, il s'agit de TCP/IP. Sans entrer dans le détail (pourtant passionnant), ce protocole indique que les adresses des ordinateurs connectés au réseau doivent avoir une adresse IP unique pendant une session. Les adresses IP sont convention-nellement construites de la façon suivante : w.x.y.z où w, x, y et z sont des octets, c'est-à-dire des entiers entre 0 et 255 (ex. : 194.98.200.22. Ne cherchez pas, c'est celle du serveur de la CNIL)

En ce qui vous concerne, cette adresse IP peut vous être attribuée de différentes manières selon votre abonnement Internet. Si vous êtes un particulier, c'est probablement une adresse différente qui vous est attribuée à chaque connexion par votre fournisseur d'accès. On parle d'adresse IP dynamique. Si vous êtes dans une entreprise ou un organisme plus lourd (université), vous avez peut-être une adresse IP définitive. On parle alors d'adresse IP fixe. Le serveur, lui, a nécessairement une adresse IP fixe (à quelques exceptions près).

« Certes, direz-vous, mais lorsque j'écris l'adresse d'un site web, je ne saisis pas d'adresse IP. Je tape des noms plus clairs, comme www. cnil. fr. Comment mon ordinateur trouve-t-il l'adresse IP de ce serveur ? »

Tout simplement en exécutant une requête auprès d'un serveur DNS, c'est-à-dire un serveur spécial destiné à retrouver les adresses IP qui correspondent à des noms de domaines (www.cnil.fr est un nom de domaine). On dit que le serveur DNS fait la « résolution » (conversion) des noms de domaines en adresses IP. La seule adresse IP dont vous ayez réellement eu besoin, c'est l'adresse IP d'un serveur DNS, généralement celui de votre fournisseur d'accès. C'est l'un des paramétrages de votre ordinateur que vous avez dû faire lorsque vous avez pris votre abonnement auprès de votre fournisseur d'accès, à moins que ce paramétrage n'ait été fait automatiquement par un programme spécifique (diffusé sur CD-ROM) comme le font désormais de nombreux fournisseurs d'accès grand public, ou encore par l'informaticien de votre entreprise. Une fois que votre ordinateur connaît l'adresse IP de votre DNS, il se charge lui-même de ces requêtes de résolution de nom de domaine.

À chacune de vos requêtes, votre navigateur lance une requête au serveur DNS, récupère l'adresse IP du serveur auquel vous demandez une page et contacte ce serveur.

c) Des paquets

Par ailleurs, le protocole TCP/IP organise la circulation des informations sur Internet en divisant les flux en paquets. Cette méthode permet d'optimiser considérablement les transactions. Par exemple, si une erreur s'était glissée quelque part dans le flux de 0 et de 1 qui compose le fichier de 3 Mo que vous avez demandé à un serveur, il faudrait attendre la fin du téléchargement pour s'en rendre compte et tout recommencer. Ce serait extrêmement long et coûteux en ressources du réseau. Avec TCP/IP, l'intégrité de chaque paquet peut être vérifiée dès qu'il arrive et s'il contient une erreur, seul ce paquet sera redemandé au serveur. Gain considérable. Et ce n'est qu'un exemple des avantages de cette méthode.

d) Un paquet pour le 22 à Asnières

Au début de chacun de ces paquets figurent des informations indispensables à la transaction, parmi elles :

- l'adresse IP de l'ordinateur qui a émis le paquet ;
- l'adresse IP de l'ordinateur auquel il est destiné.

Ces deux informations sont indispensables à toute communication sur Internet.

Soyons extrêmement clairs : peu importe ce que vous faites : web, ftp, newsgroup, messagerie, gopher, telnet, messagerie en direct (« chat »), radio en ligne (de type « real audio »}, téléphonie, jeux vidéos multijoueurs ou n'importe quoi d'autre, sur un réseau TCP/IP, tous les paquets que vous envoyez et que vous recevez contiennent votre adresse IP et celle du serveur.

e) Comment voir les paquets ?

Encore un détail : n'essayez pas de chercher dans votre navigateur les paquets en question.

On représente généralement l'architecture d'un protocole en couches. Tout en bas, la couche matérielle correspond (schématiquement) aux câbles et aux cartes utilisés (ethernet par exemple), puis la couche réseau gère la circulation des paquets à travers le réseau (IP), la couche transport gère le flux de données entre deux machines (TCP), enfin, la couche supérieure, la couche applicative, gère les détails de communication d'une application particulière entre le serveur et le client (HTTP, par exemple, si vous êtes « sur le web », ou bien FTP, pour le transfert de fichiers).

Lorsque vous utilisez votre navigateur web—qui en termes techniques n'est autre qu'un client HTTP qui dialogue avec un serveur HTTP — les informations que vous pouvez éventuellement obtenir grâce à lui sur la façon dont s'opère la transaction proviennent de la couche applicative, puisque c'est à ce niveau-là que fonctionne votre navigateur. Pour accéder aux informations des couches inférieures, il faut des logiciels capables d'analyser ces informations. Vous ne verrez donc jamais dans votre navigateur les paquets et les informations d'adresse qui les composent. En revanche, il existe des logiciels d'analyse de réseau, plus ou moins évolués, qui permettent de mieux observer les couches inférieures.

g) Un peu d'imagination

Revenons à notre transaction.

Nous sommes « sur le web » (expression imprécise signifiant en réalité : nous disposons d'un logiciel applicatif client HTTP et nous souhaitons entrer en relation avec un serveur HTTP). Vous cliquez sur un lien. Votre navigateur envoie au site web une requête constituée de paquets, chacun d'entre-eux étant précédé de votre adresse en tant qu'émetteur et de celle du serveur en tant que récepteur, paquets dont le contenu indique « envoie-moi la page située à l'adresse www. toto. com/exemples/toto. html ». Certes,

le serveur va servir cette requête, mais rien ne l'empêche, dans le même temps, d'enregistrer dans un fichier, la date, l'heure, l'adresse IP de l'ordinateur qui a fait la requête, et quel fichier a été envoyé. Absolument rien. Et si personne ne vous l'indique par ailleurs, vous ne saurez jamais qu'un tel enregistrement a été fait.

Après cela, traiter et exploiter ces enregistrements n'est plus qu'une question d'organisation et d'utilité.

Un exemple : pourquoi ne pas rassembler ces informations, les classer chronologiquement et les présenter à l'internaute comme nous le faisons en haut de cette page. Pour cela, il nous suffit de récupérer votre adresse IP via la variable d'environnement que le navigateur nous envoie et de rechercher dans notre fichier d'audit les entrées qui la comportent.

Un enregistrement du fichier d'audit, en l'occurrence le plus récent vous concernant, se présente ainsi :

Connexion le :	06/Apr/1998 à 09:29:26
Requête :	GET /traces/demonst/demo.htm HTTP/1.0
Réponse du serveur :	Ok
Volume transféré :	2355
En provenance de :	http://www.cnil.fr/traces/traces.htm
Navigateur utilisé :	Mozilla/4.02 [en] (Win95; 1)

Nous n'avons fait que l'analyser pour le présenter plus agréablement lors de la démonstration.

Cette technique n'est pas parfaite. Elle peut être mise en échec volontairement ou involontairement par l'internaute.

Enfin, il faut savoir que le fichier constitué à l'aide de cette fonctionnalité de traçage des adresses IP peut être enrichi durant votre session si vous fournissez vous-mêmes des informations : si vous remplissez un formulaire, toutes les informations que vous envoyez peuvent être associées à votre adresse IP. Si vous avez envoyé votre nom, votre adresse IP devient une étiquette parfaite. *Idem,* si vous avez envoyé un simple message électronique.

g) Plus techniquement

Nous utilisons un script CGI qui a pour but d'analyser le fichier d'audit du serveur www.cnil.fr.

Dans un premier temps, le CGI récupère votre adresse IP ou votre adresse DNS si elle est définie. Il extrait ensuite du fichier d'audit du serveur toutes les requêtes effectuées par une machine ayant la même adresse IP ou adresse DNS.

Il ne reste plus ensuite qu'à formater certaines informations contenues dans ces requêtes. Ces informations sont : la date et l'heure de connexion, la méthode utilisée pour la requête (« GET », « POST »,...), l'objet demandé (page, image, fichier, etc.), la réponse que le serveur a fourni au client, le volume en octets transférés entre le serveur et le client, la page de provenance de l'utilisateur lorsqu'il a fait sa requête et enfin la signature du navigateur qui a effectué la requête.

Pour la réponse que le serveur a fourni au client, le script CGI utilise une table de correspondance entre les codes numériques renvoyés et leur signification.

Les enjeux des fichiers d'audit

a) À quoi servent les fichiers d'audit ?

Collecter les requêtes reçues sur un serveur s'appelle habituellement « auditer » des événements. En principe, l'audit doit permettre à l'administrateur du serveur de connaître avec précision la répartition des charges du système : quand le serveur est-il le plus mis à contribution ? Quels fichiers sont les plus téléchargés ? Par exemple, si l'audit montre que le fichier toto. html est extrêmement demandé, peut-être sera-t-il amené à le concevoir différemment, pour raccourcir son temps de chargement. Si le fichier exemple, html, qui pourtant était accessible depuis la page d'accueil du serveur, est peu demandé, peut-être convient-il de revoir son ergonomie...

L'audit a donc pour finalité d'optimiser le fonctionnement du site. Il s'agit d'ailleurs d'une fonctionnalité que l'on trouve dans de nombreuses applications. Tracer des événements est, par exemple, un moyen élémentaire pour retrouver des erreurs dans un programme ou isoler des dysfonctionnements.

b) Une fonctionnalité de maintenance informatique détournée ?

Une des caractéristiques de l'audit, c'est que l'internaute n'a absolument aucune prise sur lui. Il ne peut pas deviner qu'on enregistre ses transactions. Le traçage en lui-même, tout comme le traitement du fichier ainsi constitué (tris, croisements) peut être réalisé entièrement à son insu. Dès lors, comment deviner l'utilisation qui sera faite de ce fichier ? Impossible.

Dans quelles circonstances de tels fichiers sont-il habituellement utilisés ? En temps normal, il est courant que l'administrateur du serveur tente de perfectionner le fonctionnement de son système en analysant les connexions effectuées. Dans ce contexte, il n'a pas de raison de conserver ces listes de connexions qui peuvent d'ailleurs devenir extrêmement volumineuses. Il détruira donc périodiquement les fichiers devenus obsolètes. Dans les périodes durant lesquelles une optimisation n'aura pas été programmée, il désactivera la fonctionnalité d'enregistrement, devenue inutile et par ailleurs assez gourmande en ressources, par exemple en espace disque.

Il aura cependant toujours les moyens d'observer et d'enregistrer le contenu de vos requêtes sur le serveur qu'il administre.

Mais vous avez sans doute compris qu'un tel outil peut également être utilisé à d'autres fins que purement techniques.

Par exemple, c'est à partir de cette fonctionnalité que l'on peut tenter de mesurer l'audience d'un site, de produire des statistiques en vue d'un meilleur positionnement ou d'une meilleure organisation. Où est l'atteinte aux libertés dans cet exemple ? Certainement pas dans le fait de produire des statistiques mais dans la capacité d'utiliser à cette fin des informations relatives à votre comportement sans que vous le sachiez ni que vous puissiez vous y opposer.

À ce point de notre démonstration, que faut-il penser exactement ? Certains diront sans doute « et alors ? Que peut faire un informaticien avec mon adresse IP et les pages que j'ai consultées ? Il n'a pas mon nom, il ne sait pas où j'habite ni qui je suis vraiment, c'est là l'essentiel ».

Les informations fournies par l'audit sont-elles si anodines ? Lorsque l'internaute utilise une adresse IP fixe, elle identifie de façon unique et permanente son ordinateur et très souvent son utilisateur. Dans ce cas, tout ce que vous faites peut être mémorisé et mis en relation d'une session à l'autre sur le serveur. Ces informations vous décrivent soit dans votre vie privée, soit dans votre vie professionnelle, selon que vous utilisez Internet chez vous ou dans le cadre de vos activités professionnelles. Elles peuvent être échangées, rapprochées, croisées. Cédées à qui ? Exploitées à quelles fins ? Si cette adresse

appartient en fait à l'entreprise où l'organisme qui vous emploie, que se passera-t-il si c'est à votre employeur que ces informations sont retournées ?

Quand l'adresse IP de l'utilisateur est dynamique, c'est-à-dire donnée automatiquement par le fournisseur d'accès à chaque connexion et donc différente à chaque nouvelle session, si elle n'identifie pas l'internaute, elle identifie son fournisseur, au même titre que le numéro minéralogique d'une voiture de location identifie le loueur. Facile alors de retrouver, en passant par le loueur, c'est-à-dire le fournisseur d'accès, le lien jusqu'à vous. Si votre fournisseur conserve un journal des connexions, il saura, lui, qui a eu telle adresse IP tel jour, de telle heure à telle heure. Et votre anonymat sur Internet ne sera plus qu'un souvenir !

Imaginons que vous souhaitiez aller consulter le site d'un syndicat auquel vous souhaitez adhérer, d'un parti politique dont vous vous sentez proche, d'un centre de recherche sur une maladie invalidante dont vous ou un de vos proches est atteint, d'une religion, d'un groupe de pensée...

Si les informations récupérées ne sont pas forcément très riches, elles peuvent néanmoins être habilement exploitées pour peu que lors de la connexion vous ayez été amené à en fournir d'autres de votre propre chef. Ainsi, si vous envoyez un message pendant votre connexion au serveur ou remplissez un formulaire comportant des informations plus précises sur vous, le lien entre votre adresse IP et les informations que vous avez saisies peut être fait sans difficulté et sera valide soit pour cette session dans le cas d'une adresse IP dynamique, soit en permanence dans le cas d'une adresse IP fixe. Sachez que lorsque vous donnez une information personnelle, elle peut permettre de faire le lien avec l'ensemble de votre parcours sur le serveur auquel vous fournissez l'information et donc conduire à la fabrication d'un profil précis.

Par exemple, si vous déambulez dans une galerie marchande virtuelle, chaque commerçant que vous consultez a peut-être en main le trajet que vous avez suivi auparavant. Il pourrait, par exemple, modifier son discours ou son offre en fonction de votre trajet précédent ou de votre profil s'il a réussi à maintenir un lien sur vous (par un « cookie » ou en exploitant votre adresse IP fixe si vous en avez une).

Imaginez un instant que le site en question ait un contenu d'ordre politique, religieux ou médical. Vous n'avez pas forcément envie que le serveur conserve la trace du chemin que vous avez suivi sur le site, qui peut être très révélateur de vos attentes.

Dans le cas des « newsgroups », chaque fichier consulté est encore plus significatif que les sites web visités. Si vous avez l'habitude d'aller lire les « newsgroups », même sans y participer, sachez que le serveur qui héberge les « newsgroups » peut, techniquement, savoir exactement la liste des « newsgroups » et le nombre de messages que vous avez consultés depuis votre première connexion, voire plus si l'administrateur met en place des fonctionnalités d'audit plus élaborées. Quelle source pour l'enrichissement d'une base de données de marketing ! Ou bien pour la persécution de dissidents dans des pays autoritaires...

On perçoit aisément la nécessité pour chacun de la prise de conscience que toute exploitation du fichier d'audit se situe dans le cadre légal : information des personnes, finalité claire et déclarée, droit d'opposition, droit d'accès, etc.

Un dernier point sur l'utilisation potentielle de tels fichiers, sans doute le plus justifié : dans le cas d'une procédure judiciaire, l'exploitation du fichier d'audit est un moyen extrêmement efficace pour retrouver un internaute se livrant à des activités illicites (piratage, propos interdits par la loi, etc.). Car si un fournisseur d'accès (ou votre administrateur réseau, dans le cas d'un réseau d'entreprise connecté à Internet) a conservé un fichier d'audit contenant la liste des adresses IP qui ont été attribuées à chaque connexion et que le serveur a tracé la session de chacun, il suffira au magistrat de faire saisir directement ces fichiers pour identifier par un simple rapprochement la personne recherchée.

c) On en trouve ailleurs que sur le web

Ce qu'il faut à tout prix retenir de cette démonstration, ce n'est pas tant le fait que sur le web, vos transactions avec le serveur peuvent être enregistrées. À y regarder de plus près, cela paraît logique ! C'est surtout le principe du fichier d'audit, car ce principe se retrouve absolument partout en informatique : toute application informatique peut enregistrer ce qu'elle est en train de faire dans un fichier, en y incluant la date et l'heure et a *fortiori,* les informations qui lui parviennent d'un autre ordinateur.

Sur Internet toutes les applications serveurs en sont capables : FTP, conversation (« chat »}, « newsgroups », messagerie, radio en ligne... Tout peut être « tracé » par le serveur.

Mais plus généralement, lorsque vous utilisez un logiciel, tout particulièrement s'il fonctionne en réseau, sachez que tout peut laisser une trace.

Attention : il s'agit d'une fonctionnalité, elle n'est pas nécessairement activée. Et si elle l'est, c'est peut-être purement pour des raisons d'optimisation technique, sans utilisation ultérieure ni conservation des informations ou tentative d'identification plus approfondie. Les mauvaises intentions ne doivent pas être présumées. En revanche, seule une exacte information des internautes et la transparence exigée en Europe par les lois de protection des données personnelles et en France par la loi au 6 janvier 1978, peuvent permettre de s'assurer que la vie privée et les libertés sont respectées.

(es *limites des fichiers d'audit*

Le seul cas dans lequel vous pouvez échapper aux fichiers d'audit, c'est lorsque l'administrateur du serveur a décidé de ne pas exploiter cette fonctionnalité. S'il ne vous trace pas, vous n'êtes pas tracé ! Si ce n'est pas le cas, il est impossible d'y échapper totalement car le fonctionnement du protocole TCP/IP rend indispensable l'utilisation d'adresse IP lors de l'échange d'information entre vous et le serveur. Cependant, il est possible de faire en sorte que les informations collectées par le serveur ne correspondent pas à votre ordinateur, un intermédiaire substituant alors son adresse IP à la vôtre. C'est le cas lors de l'utilisation d'un « firewall » ou d'un serveur de proxy. Mais ces solutions ne font que remonter d'un cran la conséquence : ce que ne peut plus faire l'administrateur du serveur auquel vous accédez, l'administrateur du proxy ou du « firewall », lui, le peut.

Vous pourriez également utiliser les services d'un site d'anonymisation. Mais un tel site ne vous anonymiserait que pour le serveur final. L'anonymiseur, lui, pourrait parfaitement vous tracer.

Il reste un cas classique dans lequel il est beaucoup plus difficile de vous retrouver, c'est lorsque vous effectuez votre connexion d'un cybercafé ou d'une borne publique d'accès à Internet. Là, même si tout le dispositif d'audit est en place, comment savoir qui a utilisé cet ordinateur à ce moment là ? Il faudrait avoir placé l'établissement sous surveillance...

Des traces sur votre ordinateur

Démonstration

Chacune des pages que vous consultez laisse probablement des traces sur votre ordinateur.

Si vous cliquez sur le lien correspondant à votre configuration, une fenêtre s'ouvrira sur le répertoire qui contient les fichiers caches gérés par votre navigateur. Si votre configuration ne contient pas de lien, vous devez vous-même accéder au répertoire indiqué en utilisant les outils habituels de votre système d'exploitation.

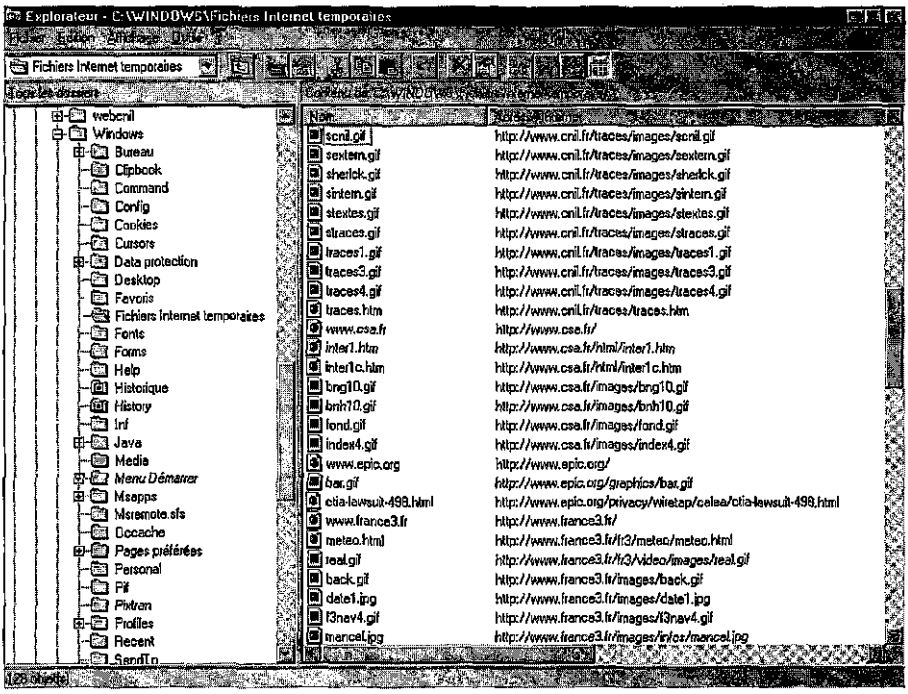


Figure 9 : Les fichiers cache sont générés par le navigateur pour op imiser les transactions. Mais ils constituent aussi une trace possible de tous vos mouvements sur Internet... jusqu'à ce que vous les ayiez supprimés I

— Emplacement des fichiers cache pour **Microsoft Internet Explorer**

Système d'exploitation	Répertoire
Windows 95	C:\Windows\Temporary Internet Files\
Windows NT	C:\WinNt\Temporary Internet Files\
Unix	//home/.rnicrosoft/TempInternetFiles *home :* Chemin d'accès à votre répertoire personnel.
Macintosh	Disque Dur:Dossier Système:Préférences:Explorer:Temporary Files

— Emplacement des fichiers cache pour **Netscape Navigator/Communicator**

Navigateur	Système d'exploitation	Répertoire
Navigator	Windows 95	C:\Program Files\Netscape\Navigator\Cache
Navigator	Windows NT	C:\Program Files\Netscape\Navigator\Users\name\Cache name : "Default" ou nom d'utilisateur
Communicator	Windows 95 Windows NT	C:\Program Files\Netscape\Communicator\Users\name\Cache *name :* "Default" ou nom d'utilisateur
Navigator	Unix	*/home/* .netscape/cache
Communicator Navigator Communicator	Macintosh	*home :* Chemin *d'accès à* votre répertoire personnel. Disque Dur:Dossier Système:Préférences:Netscape f:Cache f

La fenêtre qui vient de s'ouvrir sur votre écran vous montre les fichiers du répertoire que votre navigateur utilise comme fichiers temporaires ou « cache ». Si vous les triez dans l'ordre chronologique, toutes vos connexions les plus récentes y figurent, aussi bien les pages HTML que les images qui les composent. Pour vous en assurer, ouvrez les fichiers présents dans ce répertoire... Ce sont des résidus de vos connexions antérieures !

D'autres traces sont laissées sur votre ordinateur par les « cookies ».

Cette page montre des traces laissées par votre navigateur sur votre ordinateur.

Si cette démonstration n'a pas fonctionné, voici peut-être pourquoi.

Pourquoi ça n'a pas marché ?

Si vous n'avez pas eu accès à la liste de vos fichiers caches, c'est peut-être :

- soit que votre navigateur n'exploite pas cette fonctionnalité : qu'elle ne soit pas prévue dans le produit ou que vous l'ayez désactivée ;
- soit que ces fichiers caches sont situés dans un autre répertoire que le répertoire par défaut, auquel cas il vous suffit de chercher sur votre disque dur quels fichiers ont été créés lors de votre session ;
- dans le cas des produits Netscape, vous avez peut-être installé le navigateur ailleurs que dans le répertoire par défaut ;
- Javascript n'est peut-être pas activé sur votre navigateur.

Comment ça marche ?

Pour vous montrer quelles traces vous laissez sur votre ordinateur de vos connexions Internet, nous créons simplement un lien vers une adresse locale, située sur votre PC. À vous d'ouvrir les fichiers pour en vérifier le contenu.

a) Quelques explications simples

L'utilisation de mémoire cache est un moyen astucieux pour optimiser les temps de chargement et désengorger le réseau. Si cette fonctionnalité est présente sur votre navigateur et que vous ne l'avez pas désactivée, lorsque vous lancez une requête, votre navigateur commence par aller voir sur un répertoire de votre disque dur si la page HTML demandée n'aurait pas déjà été chargée auparavant. Si ce n'est pas le cas, il effectue la requête mais lorsque son résultat arrive, il l'enregistre sur votre disque en même temps qu'il le présente à l'écran. La fois suivante, si la même requête est lancée à nouveau, il ira simplement la lire sur votre disque. Vous verrez alors le résultat s'afficher beaucoup plus vite que s'il avait parcouru la distance réelle qui vous sépare du serveur.

Les navigateurs récents permettent de modifier certains paramètres de fonctionnement de la mémoire cache [1]. Vous pouvez notamment indiquer combien d'espace disque elle peut utiliser au maximum, ou encore si le navigateur doit vérifier si la page en question a été modifiée entre temps sur le serveur. Vous pouvez modifier le répertoire cache par défaut voire même inhiber totalement la fonctionnalité ou vider le répertoire qui contient les fichiers. De toute façon, vous pouvez toujours effacer ces fichiers à la main.

L'utilisation de mémoire cache n'est pas l'apanage des navigateurs Internet. Des microprocesseurs jusqu'aux systèmes d'exploitation, cette technique est largement employée. Elle revient à stocker plus près une information qui sera probablement redemandée ultérieurement afin de n'aller la chercher plus loin qu'une seule fois et donc d'optimiser son chargement. C'est exactement ainsi que fonctionne un proxy chez votre fournisseur d'accès ou dans votre entreprise, par exemple.

1 Mémoire cache ne signifie pas mémoire cachée. Si le terme vient à l'origine du français, il a été anglicisé et a perdu son sens d'origine avant de nous revenir sans accent !

b) Plus techniquement

Pour ouvrir une fenêtre sur le répertoire de vos fichiers caches, nous ne faisons qu'un simple lien vers une URL locale, c'est-à-dire située sur votre ordinateur. Un Javascript permet d'ouvrir la fenêtre. Le serveur ne peut absolument pas avoir accès par ce moyen au contenu de ce répertoire. Il ne fait que l'afficher pour vous.

[es *enjeux de la mémoire cache*

a) À quoi sert la mémoire cache ?

Tout simplement à optimiser les transactions. Il n'y a pas grand chose à ajouter !

b) Faut-il s'en méfier ?

Nous avons regroupé sous l'expression « mémoire cache » deux techniques différentes : la mémoire cache utilisée par votre navigateur et qui est donc stockée sur votre ordinateur et la mémoire cache utilisée par votre fournisseur d'accès (ou votre entreprise) dans le cadre d'un serveur de proxy, mémoire qui est contenue dans les disques dur de l'ordinateur qui exécute le serveur de proxy en question.

• Sur votre ordinateur :

En enregistrant dans un répertoire cache sur votre ordinateur les pages consultées, le navigateur laisse Une trace de votre passage. Certes, cette trace est précisément sur votre ordinateur et non sur le serveur. Le serveur, d'ailleurs, ignore totalement si vous en faites usage. Mais si vous pensiez effectuer une consultation discrète d'un site web, par exemple, sur l'ordinateur que vous utilisez sur votre lieu de travail ou sur un poste en accès libre, sachez que si la fonctionnalité de mémoire cache est activée, il suffit de passer après vous sur le poste, d'ouvrir le répertoire qui contient les fichiers cache et de les classer en un clic par ordre chronologique pour reconstituer entièrement votre parcours et même visualiser les pages que vous avez vous-même consulté.

Dans le même registre, la touche « bis » de votre téléphone peut aussi vous trahir. Mais elle ne dévoilera jamais que le numéro de téléphone de votre dernier correspondant. Le répertoire qui contient les fichiers cache est autrement plus prolixe !

Il n'y a donc pas de raison de se méfier de la mémoire cache dès lors qu'on n'a, comme il se doit, « rien à cacher ». Mais l'essentiel est de savoir qu'une trace particulièrement explicite de votre passage *est* imprimée derrière vous et peut être consultée. Libre à vous, alors, de la négliger ou de prendre un soin particulier à son effacement.

• Sur un proxy :

S'agissant du proxy situé chez votre fournisseur d'accès ou dans votre entreprise, qui n'est autre qu'un serveur de mémoire cache, il pose un problème plus difficile à résoudre dans la mesure où il lui est toujours possible de conserver la trace des requêtes effectuées par ses clients. Bien entendu, si vos requêtes passent par le proxy, vous n'avez pas de prise sur la conservation éventuelle de ces fichiers d'audit. À vous de décider si vous souhaitez réellement passer par ce proxy.

Les *limites de la mémoire cache*

a) Sur votre ordinateur

Vous pouvez toujours avoir un minimum de prise sur l'ordinateur que vous utilisez. Pour commencer, vérifiez dans l'écran de paramétrage de votre navigateur si une fonctionnalité de mémoire cache (également appelée « Fichiers Internet temporaires ») est présente et activée. Si ce n'est pas le cas, il est probable que votre navigateur ne crée pas de fichier cache.

Si cette fonctionnalité est présente, peut-être pouvez-vous la désactiver. Aucun fichier cache Internet ne sera laissé sur votre ordinateur. Si votre navigateur ne prévoit pas que vous puissiez désactiver l'enregistrement en cache de votre session, le seul moyen

qu'il vous reste est de procéder à votre session sans oublier, après vous être déconnecté, effacer le contenu du répertoire qui contient les fichiers (il sont généralement très nombreux car chaque image figurant dans une page web est un fichier séparé). b) Sur le proxy de votre entreprise ou de votre fournisseur d'accès

À moins d'exiger de la part de votre fournisseur d'accès plus de transparence dans l'utilisation qu'il fait de son proxy, rien ne vous permet de savoir si l'administrateur a mis en place un fichier d'audit du proxy. Si c'est le cas, il peut lui aussi conserver une trace exacte de votre connexion.

Cependant, il est très facile de contourner un proxy qui vous trace : il suffit de supprimer, dans les paramétrages de votre navigateur, les informations relatives au proxy. Rappelez-vous qu'un proxy n'est autre qu'un serveur et que votre navigateur doit disposer de son adresse pour pouvoir dialoguer avec lui. Cette adresse a donc nécessairement été entrée dans votre navigateur afin que les requêtes lui soient envoyées à lui plutôt qu'au serveur directement. Si vous supprimez ces informations, ou si vous indiquez au navigateur que vous ne souhaitez plus utiliser le proxy, vos requêtes iront directement aux serveurs. Ceci ne rendra pas impossible un traçage de vos connexions par le fournisseur d'accès. Il ne pourra simplement pas utiliser le proxy à cette fin.

En contrepartie, vos requêtes ne seront plus optimisées et vous sentirez sans doute une baisse dans les performances de votre connexion.

Pour être complet, signalons que les navigateurs de dernière génération vous permettent, tout en utilisant le proxy de votre fournisseur d'accès (ou de votre entreprise), d'indiquer une liste d'adresses de sites pour lesquelles les requêtes ne passeront pas par le proxy. Outre qu'elle laisse une trace sur votre ordinateur, cette fonctionnalité peut vous permettre un minimum de discrétion sur certains sites que vous considérez comme sensibles.

LES AUTRES ENJEUX

Les autres moyens de pistage

Les « *newsgroups* » *ont de la mémoire*

Vous connaissez sans doute les « newsgroups ». Peut-être saviez-vous que tout comme pour le web, certains serveurs ont constitué des bases de données de ces « newsgroups » et vous permettent de rechercher dans le texte intégral de toutes les interventions courantes et passées. Ce sont des moteurs de recherche sur les « newsgroups ». Jusque-là, rien de particulier. Mais certains de ces serveurs utilisent également comme entrée de leur index l'adresse e-mail des personnes qui sont intervenues sur les « newsgroups ». Prenons un exemple : comme vous utilisez beaucoup Internet et que vous êtes très ouvert sur le monde, vous posez sur les « newsgroups » des questions sur des sujets divers, vous participez aux débats, disons, en politique, religion, musique. Ici ou là, vous êtes intervenu dans quelques polémiques sur des sujets qui vous tenaient à cœur mais qui ne sont plus pour vous d'actualité.

Grâce à ces moteurs de recherche de « newsgroups », il est possible à partir de l'un des messages que vous avez envoyés, de récupérer toutes les autres interventions que vous avez faites sur tous les autres « newsgroups » et ainsi d'obtenir un profil assez net de vos centres d'intérêt. Il suffira après de lire chacune de vos interventions pour obtenir votre opinion détaillée sur l'ensemble de ces sujets.

Certes, si vous êtes intervenus, c'était pour être lu. Mais pas nécessairement pour que l'on puisse recouper vos différents messages. Ainsi, votre employeur, par exemple, réel ou potentiel, pourra aisément obtenir des informations que vous ne lui auriez pas forcément donné sur sa demande et qu'il n'aurait pas été forcément légal de sa part de recueillir.

Intervenir sur un « newsgroups » est un acte réfléchi qui se situe dans un contexte : les messages s'effacent relativement vite des « newsgroups », la quantité de « newsgroups » (plus de 15 000) et d'interventions pourrait vous donner à penser que les vôtres sont assez anodines. Une parmi tant d'autres ! Il est important que vous sachiez que ce n'est pas le cas et que tout comme le serveur de « newsgroups » peut tracer vos lectures de ces messages, des moteurs de bases de données accessibles à tous peuvent tracer vos interventions, les conserver aussi longtemps qu'ils le souhaitent et vous profiler à volonté.

Le fournisseur d'accès parmi les autres acteurs du réseau

Le simple bon sens permet de constater que le fournisseur d'accès Internet est le maillon le plus faible de la chaîne. Si le serveur auquel vous vous connectez peut vous tracer, il y a de grandes chances pour qu'il ne puisse jamais disposer de votre identité, à moins que vous la lui ayiez donnée lors d'une de vos connexions ou que vous disposiez personnellement d'une adresse IP fixe (cas plutôt rare).

Votre fournisseur d'accès, lui, vous connaît puisque vous lui réglez un abonnement et il a la possibilité technique de tracer l'intégralité de vos transactions. S'il doit *y* avoir une relation de confiance avec l'un des acteurs d'Internet, c'est avec lui !

S'est-il engagé à ne pas analyser les connexions ? Sinon, s'est-il engagé à utiliser ces informations pour des finalités précises et limitées ? S'est-il engagé à ne pas transmettre ces informations à des tiers ? S'est-il engagé sur une durée de conservation de ces informations ?

Rappelons que sont concernés ici non seulement les accès à des sites web, mais également l'ensemble des autres activités que vous pouvez exercer sur Internet : « newsgroups », transfert de fichiers, conversation en temps réel, téléphonie, jeux vidéo, radio en ligne, etc.

tes *autres maillons de la chaîne*

Allons un peu plus loin. Vous avez sans doute entendu parler de l'origine d'Internet : réseau créé par les militaires américains petit à petit récupéré par les universitaires, etc. De ces explications, il ressort généralement que la structure et le fonctionnement du réseau interdisent à l'un des maillons de la chaîne, l'un des routeurs ou des ordinateurs situés sur le chemin de vos paquets, de reconstituer l'intégralité de votre communication avec un serveur en analysant précisément ces paquets. Car, toujours selon ces explications courantes, à chaque routeur, le paquet IP peut prendre un chemin différent, quasi impossible à prévoir. Cette explication conforte l'idée du rôle déterminant du fournisseur d'accès qui serait alors le seul, avec le serveur, à pouvoir tout reconstituer.

Or, s'il est vrai que le chemin suivi par vos requêtes peut être différent d'une transaction à l'autre, il est inexact d'affirmer 1) qu'il est toujours différent, 2) qu'il ne peut pas être prévu. Car le réseau a été conçu pour réorienter les paquets lorsqu'une route est bloquée mais lorsque tout se passe bien, c'est le chemin optimal qui est utilisé, et ce chemin est toujours le même.

Vous pouvez le vérifier vous-même. Il existe un petit utilitaire appelé habituellement Traceroute et que l'on trouve sur tous les ordinateurs connectés à des réseaux TCP/IP (sous Windows, il s'appelle « tracert. exe ») ou que l'on peut télécharger à partir de nombreux sites. Cet utilitaire, comme son nom l'indique, trace la route que prennent vos requêtes pour atteindre un serveur distant. Lancez-le en lui indiquant une adresse très éloignée, à l'étranger. Et observez le chemin suivi par le paquet, de routeur en routeur, jusqu'à destination. Relancez le à quelques minutes ou quelques heures d'intervalles. Vous pourrez sans doute constater que votre paquet suit le même chemin. Ou plus exactement, vous en déduirez que la règle est qu'un paquet suit toujours un chemin optimal que seule l'exception lui fait changer, exception que peut constituer un problème sur ce chemin

(engorgement, machine en panne, etc.). Cela arrive, mais en règle générale, cela reste l'exception.

Il faut donc rester raisonnable et le répéter clairement : l'anonymat sur Internet nécessite des efforts (chiffrement par exemple), la surveillance aussi. Comme dans le monde réel. Et d'ailleurs Internet n'est pas ailleurs que dans le monde réel !

Tout logiciel peut comporter des failles

Tout système informatique peut contenir des failles de conception qu'un programmeur habile peut exploiter.

De telles failles de conception s'expliquent à la fois par la complexité croissante des logiciels et par la nécessité pour leurs producteurs de les lancer sur le marché très rapidement, risquant ainsi d'oublier certains tests. Vous trouverez aisément sur Internet des informations à ce sujet. Les administrateurs de systèmes informatiques se sont organisés pour lutter contre l'exploitation de telles failles de sécurité, notamment grâce au CERT de l'Université de Carnegie Melon (http : //www. cert. org/).

Ce qu'il convient de retenir, c'est que lorsqu'une faille est découverte et exploitée par un individu, elle ne tarde généralement pas à être découverte également par les autres acteurs d'Internet, notamment les administrateurs systèmes des serveurs connectés. Ils peuvent ainsi prendre les mesures nécessaires pour faire cesser cette nuisance, en commençant par informer la communauté des acteurs d'Internet.

Si certaines de ces failles ont beaucoup fait parler d'elles, force est de constater qu'il n'a pas fallu longtemps pour les rendre inopérantes. Ainsi, il est probable que le danger qu'elles représentent, s'il existe toujours, n'est pas véritablement une menace durable pour tout un chacun.

Java et activex

De nouvelles évolutions logicielles permettent aujourd'hui de faire beaucoup plus de choses à partir d'un serveur web que d'afficher des écrans d'information. Le langage Java de Sun Microsystems par exemple (à ne pas confondre avec Javascript), tout comme les ActiveX conçus par Microsoft, permet d'exécuter de véritables applications interactives originales. Certaines de ces nouvelles techniques intègrent la possibilité de manipuler des fichiers sur le PC de l'ordinateur client. Heureusement, la sécurité a été prise en compte et, pour Java par exemple, l'utilisateur a la possibilité de fixer lui-même le niveau de sécurité qu'il souhaite. Encore faut-il qu'il soit conscient et informé des tenants et aboutissants cette technique. On doit certainement exiger de la part des éditeurs de logiciels et des serveurs le plus d'information possible, mais cela ne doit pas dispenser l'internaute de faire lui-même un effort d'information.

Et dans votre entreprise ?

Internet au bureau

Il va de soi que si vous accédez à Internet dans le cadre de vos activités professionnelles, vous devez être conscients des possibilités de traçage qui existent techniquement. Selon l'architecture de raccordement au réseau choisi par l'administrateur réseau, elles peuvent être plus ou moins larges.

Ainsi, si votre accès Internet passe par un routeur, un proxy ou un « firewall » dans l'entreprise avant de partir sur Internet, beaucoup de choses sont possibles. À vous d'exiger le respect de la loi et notamment l'information des salariés. Si votre connexion passe par un simple modem raccordé à votre prise de téléphone vers un fournisseur d'accès, votre employeur n'a pas de moyen de vous pister sauf :

- à demander et obtenir ces informations du fournisseur d'accès (ce qui implique que
ce dernier vous ait pisté) ;
- à vérifier périodiquement le contenu de votre disque dur : fichiers caches, « cookies », etc.

Dans tous les cas, des règles juridiques existent que chacun, y compris vous, doit respecter.

Et intranet dans tout ça ?

Le réseau Internet revêt comme particularité de permettre à chacun de s'y connecter. On parle de réseau international ouvert. Un réseau intranet fonctionne exactement de la même façon, avec les mêmes moyens et les mêmes logiciels. La seule différence est qu'il ne s'agit pas d'un réseau ouvert. Seuls peuvent *s'y* connecter les personnes autorisées. Un réseau intranet peut être extrêmement petit (quelques PC dans une PME) ou extrêmement grand et relier, comme c'est le cas pour certains grands groupes mondiaux, des dizaines de serveurs et des milliers d'ordinateurs. Dans tous les cas, l'infrastructure est exactement la même. Par contre, le réseau étant fermé, il est beaucoup plus aisé d'y procéder à des authentifications et autres contrôles.

S'informer sur les techniques, s'informer sur le droit

Sur le lieu de travail peut-être plus qu'ailleurs, il convient d'être au fait des possibilités de traçage qu'offre la technologie. Si elles sont nombreuses, cela ne signifie pas qu'elles sont systématiquement utilisées. Le meilleur moyen d'éviter les conflits reste la transparence sur les règles appliquées dans l'entreprise ou l'organisme qui vous emploie : règles légales applicables à tous, règles internes spécifiques.

Quelle attitude adopter ?

- Rester réaliste

Sur Internet comme ailleurs, l'anonymat nécessite des efforts, la surveillance aussi. Il ne faut pas sombrer dans la paranoïa ni dans l'utopie. Internet n'est pas un monde virtuel. C'est un réseau informatique ouvert. À ce titre, lorsque vous l'utilisez, vous laissez des traces. Votre véhicule est-il invisible sur l'autoroute ? Pourquoi votre connexion sur Internet le serait-elle ? On peut vous observer, vous devez le savoir. Cela ne signifie pas que l'on vous observe. Il convient de rester vigilant et d'apprendre à mesurer les risques et à agir en conséquence.

- Exiger

Sur Internet comme ailleurs, la loi doit être respectée. Si ce n'est pas le cas, exigez-le. Les obligations qui pèsent sur les organismes qui créent ou exploitent des traitement automatisés sont les mêmes sur Internet. Vos droits également. Obligation d'information, obligation de déclaration, droit d'opposition, droit d'accès, droit de rectification, droit à l'oubli : faites respecter la loi, utilisez les recours.

Si le réseau est mis en place dans le cadre de votre lieu de travail, l'intranet doit respecter la loi. Votre employeur doit respecter ses obligations et garantir vos droits.

Des activités illégales peuvent également se déployer sur Internet, activités qui troublent l'ordre public : il est de la responsabilité de chacun, s'il en a connaissance, de les dénoncer, afin que les agissements de quelques uns ne puissent pas justifier la surveillance de tous.

- S'informer

Dans la vie quotidienne, nous prenons, sans même y penser, mille précautions pour protéger notre vie privée. Elles sont devenues naturelles. Sur Internet, tout est nouveau. Les outils évoluent tellement vite que l'on a parfois le sentiment d'être dépassé.

Il faut déjà beaucoup de temps pour apprendre à exploiter efficacement les logiciels, en reste-t-il pour s'informer des risques qu'ils font courir à notre vie privée ? Une bonne utilisation d'Internet suppose que vous ayez un comportement responsable, c'est-à-dire que vous soyez relativement conscient des conséquences de vos actes, en particulier de leurs répercussions sur l'intégrité de votre vie privée. Pour cela, restez informé.

• Participer

Si vous estimez que l'information n'est pas assez diffusée, que telle ou telle technique représente un danger méconnu, que tel projet pose un problème de ce point de vue, participez au débat. Internet est fait pour ça. Votre intervention peut peser beaucoup plus que vous ne le pensez. Votre contribution est importante.

Glossaire

Applet Java : programme envoyé par le serveur, qui s'exécute grâce à un interpréteur Java intégré à votre navigateur. Une applet Java peut exécuter des opérations extrêmement puissantes. La programmation en langage Java en est d'autant plus complexe.

CGI (Common Gateway Interface) : langage de script exécuté sur le serveur qui permet de manipuler des données avant de les renvoyer à l'ordinateur client. C'est généralement un script CGI qui gère les données issues des formulaires que vous pouvez envoyer à partir d'une page web.

Cookie : voir Qu'est-ce qu'un « cookie » ?

FTP (File Transfer Protocol) : protocole de transfert de fichiers. Ensemble de conventions qui définissent les règles (protocole) permettant à un serveur FTP de dialoguer avec un client FTP (les navigateurs récents sont tous clients FTP en même temps que clients HTTP). Un serveur FTP permet à un client d'écrire ou de lire des fichiers sur le (ou à partir du) serveur.

HTML (HyperText Markup Language) : langage de description de pages dont les deux caractéristiques principales sont :
- la navigation hypertextuelle grâce aux liens ;
- le multimédia (intégration de textes, d'images, et de sons). Le navigateur lit la page HTML, interprète les balises et les liens et l'affiche sur votre écran. Vous pouvez probablement voir la page HTML source à partir du menu affichage de votre navigateur.

HTTP (HyperText Transfert Protocol) : protocole grâce auquel un client web et un serveur web peuvent dialoguer.

Javascript : langage de script intégré dans une page HTML et qu'exécute votre navigateur lorsqu'il lit et affiche la page HTML. Le langage Javascript est relativement simple mais peu puissant.

Serveur DNS (Domain Name Server) : serveur de nom de domaine. C'est lui qui converti des noms de domaines (ex. : www. cnil. fr) en adresses IP (ex. : 194.98 200.22). Le serveur DNS que vous utilisez est généralement situé chez votre fournisseur d'accès.

URL (Uniform Ressource Locator) : adresse d'une ressource web. L'URL s'écrit de la façon suivante : protocol : //server/directory/document, par exemple : http : //www. cnil. fr/essai/essai. html. Elle peut être complétée par des paramètres précédés d'un « ? ».

Annexe 7

Décisions des juridictions

ARRÊT DU CONSEIL D'ÉTAT, 6 JANVIER 1997

Vu la requête enregistrée le 7 juin 1994 au secrétariat du contentieux du Conseil d'Etat, présenté par M. M. B., agissant comme représentant légal de la Caisse d'épargne Rhône Alpes Lyon dont le siège est 42, boulevard Eugène Deruelle à Lyon (69003) ; la Caisse d'épargne Rhône Alpes Lyon demande au Conseil d'État d'annuler pour excès de pouvoir :

1) la décision en date du 15 juillet 1993, par laquelle la Commission nationale de l'informatique et des libertés (CNIL) a refusé de délivrer récépissé de la déclaration déposée par la Caisse d'épargne Rhône Alpes Lyon le 25 juin 1993 ;

2) la décision née du silence gardé pendant plus de quatre mois par ladite commission suite au dépôt d'une nouvelle déclaration transmise à la commission le 7 décembre 1993 ;

Vu les autres pièces du dossier ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

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 ;

Après avoir entendu en audience publique :

- le rapport de M., maître des requêtes ;
- les conclusions de M., commissaire du gouvernement ;

Sur la compétence du Conseil d'État :

Considérant qu'aux termes de l'article 2 du décret susvisé du 30 septembre 1953 : « Le Conseil d'État reste compétent pour connaître en premier et dernier ressort :... 6° — Des recours en annulation dirigés contre les décisions administratives des organismes collégiaux à compétence nationale »... ; que la Caisse d'épargne Rhône Alpes Lyon demande au Conseil d'État d'annuler pour excès de pouvoir, d'une part, la décision en date du 15 juillet 1993 par laquelle la Commission nationale de l'informatique et des libertés a refusé de lui délivrer le récépissé de la déclaration qu'elle avait déposée le 25 juin 1993, en application de l'article 16 de la loi susvisée du 6 janvier 1978, en vue de la mise en oeuvre d'un traitement automatisé d'informations nominatives, d'autre part, la décision née du silence gardé pendant plus de quatre mois par ladite commission comme suite au dépôt d'une nouvelle déclaration transmise à la commission le 7 décembre 1993 ; que le Conseil d'État est compétent pour connaître, en premier et dernier ressort, de la demande d'annulation dirigée contre la décision en date au 15 juillet 1993, laquelle émane d'un organisme collégial à la compétence nationale et qu'il est, par suite, également compétent pour connaître des conclusions connexes dirigées contre la décision implicite rejetant la nouvelle déclaration de la Caisse d'épargne Rhône Alpes Lyon, déposée auprès de la Commission nationale de l'informatique et des libertés le 7 décembre 1993 ; que celle-ci n'est pas fondée à soutenir que l'affaire devrait être attribuée au tribunal administratif de Paris ;

Sur la fin de non-recevoir opposée par la Commission nationale de l'informatique et des libertés :

Considérant que le moyen présenté au soutien de cette fin de non-recevoir, et tiré de ce que M. M. B., président du directoire, n'aurait pas produit le mandat l'habilitant à représenter la Caisse d'épargne Rhône Alpes Lyon dans le présent litige manque en fait ; que, dès lors, la Commission nationale de l'informatique et des libertés n'est pas

fondée à soutenir que la requête présentée pour la Caisse d'épargne Rhône Alpes Lyon serait irrecevable ;

Sur la légalité des décisions attaquées :

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

Considérant qu'aux termes de l'article 16 de la loi susvisée du 6 janvier 1978 : « Les traitements automatisés d'informations nominatives effectués pour le compte des 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 oeuvre le traitement. Il n'est exonéré d'aucune de ses responsabilités » ; qu'aux termes de l'article 19 de la même loi « 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 oeuvre 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 tout 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... Toute modification aux mentions énumérées ci-dessus, ou toute suppression de traitement, est portée à la connaissance de la commission... » ;

Considérant que la Caisse d'épargne Rhône Alpes Lyon a déposé, en application de l'article 16 précité, à deux reprises, une déclaration relative à la constitution d'un fichier informatisé, en vue d'offrir un livret d'épargne aux enfants dès leur naissance ;

Considérant que, s'il appartient à la Commission nationale de l'informatique et des libertés de s'assurer de la régularité de la déclaration effectuée auprès d'elle au regard des prescriptions des articles 16 et 19 précités, et notamment de ce que les précisions exigées par l'article 19 figurent dans la déclaration, il résulte des termes même de l'article 16 que la Commission ou son président ne peut refuser de délivrer récépissé du dépôt de déclaration, dès lors que le dossier présenté comporte bien l'engagement prévu à l'article 16 précisé et est conforme aux prescriptions de l'article 19 précité ; que par suite, la Caisse d'épargne Rhône Alpes Lyon est fondée à soutenir que les décisions attaquées refusant de lui délivrer récépissé, lesquelles n'étaient pas motivées par l'absence soit de l'engagement susmentionné, soit de l'un des éléments énumérés à l'article 19, sont entachées d'illégalité ;

Décide :

Article 1er : La décision de la Commission nationale de l'informatique et des libertés en date du 15 juillet 1993 et la décision implicite de rejet née du silence gardé par le président de la Commission nationale de l'informatique et des libertés sur la demande qui lui avait été adressée le 7 décembre 1993 sont annulées.

Article 2 : La présente décision sera notifiée à la Caisse d'épargne Rhône Alpes Lyon, au Premier ministre, au garde des Sceaux, ministre de la Justice et au président de la Commission nationale de l'informatique et des libertés.

Annexe 7

L'ARRET DE LA COUR D'APPEL DE VERSAILLES DU 2 JUILLET 1997

Rappel de la procédure :

Le jugement :

Par jugement en date du 7 mai 1996, le tribunal correctionnel de Nanterre a dit les dispositions de l'article R 10 du code des postes et télécommunications inapplicables en l'espèce car contraires aux dispositions des articles 86 et 90 du traité instituant la Communauté économique européenne ;

— A dit que les éléments constitutifs de l'infraction prévue et réprimée par l'article 226.18 du code pénal ne sont pas réunis ;

— A renvoyé les fins de la poursuite x et la société F. ;

— A laissé les dépens à la charge du Trésor public ;

— A déclaré en conséquence irrecevable la constitution de partie civile de France Télécom ;

— Lui a laissé la charge des dépens de l'action civile,

(Traitement d'informations nominatives malgré l'opposition légitime de la personne concernée, le 1er mars 1994, Issy-les-Moulineaux).

Appels :

Appel a été interjeté par :

- France Télécom, le 10 mai 1996,
- Le ministère public, le 17 mai 1996 ;

Madame le président a ensuite averti les parties présentes que l'arrêt serait prononcé le 2 juillet 1997, conformément a l'article 462 du code de procédure pénale.

Décision

La cour, après en avoir délibéré conformément à la loi, a rendu l'arrêt suivant :

Statuant sur les appels, relevés à titre principal par la société anonyme France Télécom et à titre incident par le ministère public, des dispositions du jugement susvisé, qui a renvoyé x et la société à responsabilité limitée F. des fins de la prévention d'avoir à Issy-les-Moulineaux courant mars 1994, en tout cas sur le territoire national et depuis temps non couvert par la prescription, procédé à un traitement d'informations nominatives concernant des personnes physiques abonnées au téléphone malgré leur opposition fondée sur des motifs légitimes.

Faits prévus et réprimés par les articles 226-18 al. 1 et 226-24 du code pénal, et par les articles 26 et 41 de la loi 78-17 du 6 janvier 1978.

Considérant, référence faite pour l'exposé des faits, aux énonciations précises et complètes du jugement entrepris et aux conclusions des parties, qu'il suffit de rappeler les éléments suivants :

La SARL F., créée en 1987 par x, a pour activité essentielle la création et la commercialisation de fichiers d'adresses, répondant aux critères de sélection spécifiés par sa clientèle, en vue d'opérations de publipostage, de télémarketing ou de sondages.

Elle utilise à cette fin diverses sources d'information, en particulier les données, notamment mises à jour, de l'annuaire électronique diffusé par réseau informatique par France Télécom, exploitant public du réseau téléphonique, mais non expurgées des noms des abonnés ne désirant pas faire l'objet d'un démarchage publicitaire, et ayant donc demandé leur inscription sur « liste orange », conformément aux dispositions des articles 26 de la loi de 1978 et R 10-1 al. 1 du code des postes et télécommunications.

Dans le but de se conformer néanmoins à la législation en vigueur, et notamment aux dispositions de l'alinéa 2 de cet article R 10-1, qui interdisent l'utilisation par

quiconque à des fins commerciales des noms de ces abonnés, la société F. a demandé à plusieurs reprises à France Télécom de lui donner les moyens d'expurger ses propres fichiers, soit en lui communiquant cette « liste orange », soit en procédant à des marquages de ses annuaires, soit en opérant les corrections nécessaires sur ces fichiers, préalablement à leur commercialisation.

France Télécom s'y étant refusé et l'ayant renvoyée à utiliser ses services Marketis et Teladress, qui commercialisent les listes d'abonnés expurgées des données litigieuses, moyennant un coût de 0,30 F par adresse, la société F., jugeant ces prix prohibitifs et anticoncurrentiels, a saisi de ce litige le tribunal de commerce de Paris, puis, ayant été déboutée de ses demandes, a déféré cette décision à la cour d'appel de Paris, laquelle a sursis à statuer dans l'attente d'une solution définitive à la présence instance.

France Télécom, qui fait grief pour sa part à la société F. de « télédécharger » dans des conditions déloyales son annuaire électronique en branchant sur son numéro d'appel « 11 », dont la durée gratuite d'utilisation est de trois minutes, des batteries d'ordinateurs programmés pour couper la communication au bout de 2 mn 59 secondes, puis la rétablir et bénéficier ainsi à nouveau de cette gratuité, et qui lui reproche de ne pas respecter l'opposition manifestée par certains de ses abonnés à la divulgation de leurs coordonnées à des fins commerciales, a en effet, de son côté, le 3 février 1994, déposé plainte auprès de Monsieur le procureur de la République de Nanterre, pour concurrence déloyale, contrefaçon et infractions à la loi « informatique et liberté ».

A l'issue de l'information ouverte sur ces faits, et au cours de laquelle il a également été instruit sur une plainte de la Commission nationale informatique et libertés (CNIL) déposée pour défaut de déclaration préalable à la mise en oeuvre d'un traitement informatique, le magistrat instructeur a constaté l'amnistie, par l'effet des dispositions de la loi du 3 août 1995, de la contravention à l'article R. 10-1 du code des postes et télécommunications, a dit non constituée l'infraction à l'article 226-16 du code pénal dénoncée par la CNIL, a estimé au contraire que l'infraction à l'article 226-18 du même code, qui réprime le fait de procéder à un traitement d'informations nominatives concernant une personne physique malgré son opposition fondée sur des motifs légitimes, était établie en tous ses éléments, et a en conséquence renvoyé x ici la société F. devant le tribunal correctionnel de ce seul chef.

Aux termes du jugement déféré, ce tribunal, faisant droit aux moyens soulevés par les prévenus pour conclure à leur relaxe, tirés notamment de l'illégalité de l'article R. 10-1 du code des postes et télécommunications au regard des articles 86 et 90 du traité de Rome, et du caractère relatif de l'opposition manifestée par les abonnés au téléphone auprès de l'exploitant public, a estimé que les dispositions de cet article R. 10-1 avaient permis à France Télécom, qui commercialise, par le biais des services Marketis et Teladress, à des prix « inaccessibles » aux entreprises, la liste des abonnés au téléphone expurgée de la « liste orange », d'abuser de sa position dominante sur le « marché pertinent » ; qu'elles étaient dès lors de plein droit inapplicables ; que, par suite, la réalité et la légitimité de l'opposition exprimée par les abonnés au téléphone à la commercialisation des données nominatives les concernant ne pouvaient découler automatiquement de cet article R. 10-1 ; qu'aucun élément du dossier ne permettait dès lors d'induire la réalité et la légitimité de cette opposition ; que les éléments constitutifs du délit de l'article 226-16 du code pénal n'étaient donc pas réunis.

Considérant que, critiquant cette motivation, et concluant à la réformation de ce jugement, la SA France Télécom prie la cour :

- de la déclarer recevable en sa constitution de partie civile visant à réparer son seul préjudice personnel et direct ;

- de lui donner acte de ce qu'elle entend réserver sa demande de réparation de son
préjudice indirect devant la cour d'appel de Paris ;
— de dire que la responsabilité de x qui dirige de nombreuses sociétés d'exploitation de fichiers, est distincte de celle de la société F. ;
— de condamner chacun des prévenus à lui verser la somme de un franc au titre de son préjudice moral ;
— d'ordonner par application de l'article 131-39 8°) du code pénal, la saisie et la destruction des données nominatives utilisées par la société F. sans l'autorisation des personnes concernées, de tous ses logiciels de télédéchargement et de ses automates d'appel ;
— d'interdire à la F., à titre complémentaire et en application de l'article *1*31-39 1 °*)* du code pénal, de procéder directement ou indirectement à tout traitement de données nominatives concernant des personnes physiques abonnées au téléphone malgré leur opposition fondée sur des motifs légitimes ;
— et de condamner la société F. à lui verser la somme de 15 000 F au titre de l'article 475-1 du code de procédure pénal.

Considérant que le ministère public requiert le rejet des exceptions de procédure, la réformation du jugement et la condamnation de x de la société F. au paiement d'une amende de 100 000 F et de 400 000 F, respectivement, ainsi qu'à la publication de la décision à intervenir dans deux journaux.

Considérant qu'in *limine litis* x conclut :
— à l'irrecevabilité de l'appel du ministère public au regard du pacte international relatif aux droits civils et politiques du 19 Décembre 1966, au motif qu'en matière pénale, le droit d'appel serait exclusivement réservé à la personne condamnée, et que l'exercice d'un tel droit par le ministère public priverait le prévenu relaxé en première instance du double degré de juridiction ;
— à l'irrecevabilité de l'appel de France Télécom, faute d'indication dans l'acte d'appel du nom du représentant légal de cette personne morale, et par suite à la « nullité » de l'appel incident du ministère public, interjeté le onzième jour suivant le prononcé du jugement entrepris ;
— subsidiairemenf à l'irrecevabilité de la constitution de partie civile de France Télécom, faute d'intérêt à agir aux lieu et place des personnes directement victimes des infractions dénoncées ;
— qu'au fond, il soutient :
2) que les dispositions de l'article R. 10-1 du code des postes et télécommunications, qui étendent à « quiconque » l'obligation de respecter l'opposition à recevoir des sollicitations commerciales manifestée auprès de France Télécom par ses abonnés, sont inapplicables en l'espèce, en ce qu'elles sont contraires aux articles 86 et 90 du traité de Rome, aux principes constitutionnels et supra nationaux consacrant l'égalité des citoyens devant la loi, la prévisibilité de la loi pénale, la liberté d'expression et la liberté du commerce, et à l'article 26 de la loi du 6 janvier 1978, dès lors notamment qu'elles permettent à l'exploitant public du réseau téléphonique, qui se réserve l'information obtenue dans le cadre de ses missions de service public, et interdit aux tiers l'accès de cette information aux mêmes conditions que celles consenties à Marketis et Teladress, d'abuser de sa position dominante sur le marché de la fourniture de données, et qu'elles privent en revanche ces tiers de la possibilité de savoir s'ils se conforment à la loi et si parmi les adresses vendues, certaines venues, certaines figurent ou non sur « la liste orange » ;
3) que sa responsabilité pénale ne peut être recherchée, dès lors que l'est celle de la société F. pour le compte de laquelle ont été commis les faits litigieux ;
4) subsidiairement, que l'infraction de l'article 226-18 du code pénal, qui exigerait la réunion de cinq éléments, à savoir l'existence d'informations nominatives et d'un traite ment de ces informations, une opposition, l'exercice du droit d'opposition auprès du

maître du traitement, et un motif légitime de s'opposer à ce traitement, n'est pas caractérisée ;
5) que l'opposition manifestée par les usagers du téléphone auprès de France Télécom ne serait pas une opposition générale à un traitement d'informations nominatives au sens de la loi de 1978, mais simplement une opposition à des sollicitations commerciales ;
6) que France Télécom refusant de fournir la liste de ces personnes, cette opposition ne pourrait être connue du maître du traitement, qui ne pourrait de surcroît apprécier la légitimité du motif invoqué ; qu'elle n'aurait donc pas de portée générale mais vaudrait seulement vis-à-vis de l'exploitant public ;
7) que la mise sur « liste orange » n'impliquerait pas *ipso facto* que l'opposition a été faite pour un motif légitime au sens de l'article 26 de la loi du 6 janvier 1978 ;
8) que l'élément matériel du délit reproché n'est donc pas établi ; que l'élément moral ou intentionnel fait également défaut ; que la preuve d'une intention de violer délibérément la loi pénale n'est pas rapportée, qu'au contraire, la volonté de respecter le droit d'opposition des personnes inscrites en « liste orange » est démontrée ;
9) très subsidiairement que l'état de nécessité créé par France Télécom qui ne laisse à ses concurrents que le choix de cesser leur activité commerciale ou d'enfreindre la loi pénale, ou à défaut l'erreur de droit, sont de nature à l'exonérer de toute responsabilité ;
10) Qu'il prie en conséquence la cour de faire droit à ses exceptions de procédure, subsidiairement de confirmer le jugement entrepris, plus subsidiairement, de surseoir à statuer dans l'attente de la décision à intervenir dans la procédure actuellement instruite au cabinet du juge d'instruction de Paris contre France Télécom pour détournement de fichiers et abus de position dominante, et encore plus subsidiairement de faire application de la loi d'amnistie du 3 août 1995.

Considérant que la société F. conclut également à l'irrecevabilité de l'appel de France Télécom et subsidiairement à celle de sa constitution de partie civile, et soulève au fond les mêmes moyens, tirés de l'absence d'élément matériel de l'infraction par suite de l'illégalité et de l'inapplicabilité des dispositions réglementaires fondant la poursuite, de l'absence d'intention frauduleuse, et subsidiairement de l'existence de causes d'irresponsabilité.

Sur ce, la cour

Considérant que la société F., qui n'a pas été régulièrement citée, faute de délivrance de l'acte à l'administrateur judiciaire désigné en application de l'article 706-3 du code de procédure pénale pour la représenter dans la présente instance, accepte de comparaître volontairement sur les faits visés à la prévention.

Sur les exceptions de procédure

Considérant que, contrairement à ce que soutient X les dispositions du pacte international relatif aux droits civils et politiques qui prévoient que « toute personne déclarée coupable d'une infraction de culpabilité et la condamnation », n'excluent pas que le ministère public, partie au procès pénal, puisse, comme le prévoit la loi, relever appel des décisions, y compris de relaxe, rendues par les juridictions répressives ; que l'exercice de ce droit d'appel n'est pas incompatible avec le principe du double degré de juridiction, dès lors qu'il permet précisément un nouvel examen des faits et de leur éventuelle imputabilité au prévenu ;

Que l'exception d'irrecevabilité de l'appel du ministère public sera donc rejetée ;

Considérant en revanche que l'appel de France Télécom, interjeté sans qu'il soit fait mention dans l'acte formalisant cet appel, du nom de son représentant légal, est irrecevable ;

Considérant que l'appel incident du ministère public a été relevé le 17 mai 1996, soit onze jours après le prononcé de la décision attaquée.

Mais considérant que le délai de 10 jours visé à l'article 502 du code de procédure pénale expirait le 16 mai 1996, jour de l'Ascension ; que s'agissant d'un jour férié, et par application des dispositions de l'article 801 du même code, qui prévoient que le délai qui expirerait un samedi ou un dimanche ou un jour férié ou chômé est prorogé jusqu'au premier jour ouvrable suivant, l'exception tirée de la prétendue tardiveté de cet appel sera rejetée.

Au fond

Considérant que les prévenus sont poursuivis sur le fondement de l'article 226-18 du code pénal qui réprime le fait de « procédera un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur un motif légitime », et de l'article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui prévoit que « toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement ».

Considérant que l'article R. 10-1 du code des postes et télécommunications dispose que :

« Les personnes physiques ayant souscrit un abonnement au service du téléphone fixe ou du télex, peuvent, en application de l'article 26 (précité) demander, sans redevance supplémentaire, à ne pas figurer sur les extraits des listes d'utilisateurs, commercialisés par l'exploitant public.

Est interdit l'usage par quiconque, à des fins commerciales ou de diffusion dans le public, des informations nominatives extraites des listes d'utilisateurs et concernant les personnes mentionnées à l'alinéa précédent.
Toutefois, ces informations peuvent être utilisées ou communiquées aux seules fins d'édition des listes d'utilisateurs mentionnées à l'article R. 10 ».

Considérant que, comme l'ont dit les premiers juges, et nonobstant les allégations contraires et intimés, il résulte de ces dispositions que le refus des abonnés du téléphone de recevoir des sollicitations commerciales constitue, dès lors qu'il tend à la protection de leur vie privée, un motif légitime d'opposition à l'utilisation des données nominatives les concernant en vue d'un traitement informatique à des fins de constitution de fichiers de prospection ;

Que l'obligation à tous de respecter l'opposition manifestée en ce sens par ces personnes auprès de l'exploitant public, sauf à encourir les sanctions prévues par l'article 226-18 du code pénal précité.

Considérant qu'il résulte de diverses plaintes formulées auprès de France Télécom, et n'est d'ailleurs pas sérieusement contesté, que la société F., qui commercialise des informations nominatives relatives aux abonnés au téléphone obtenues par connexion sur l'annuaire électronique édité par France Télécom, n'a pas procédé, préalablement à la vente des fichiers constitués à partir de ces données à sa clientèle, à l'expurgation de celles concernant les personnes inscrites en « liste orange », et qu'elle a ainsi enfreint ces dispositions.

Considérant que l'illégalité alléguée de l'article R. 10-1 susvisé du code des postes et télécommunications au regard des articles 86 et 90 du traité de Rome, qui conduirait France Télécom, seul détenteur des données publiques de l'annuaire et des informations relatives aux abonnés inscrits en « liste orange » à refuser à des entreprises concurrentes sur le marché du marketing direct, l'accès à ces informations, sauf à leur imposer de recourir à ses propres services commerciaux dans des conditions prétendument constitutives de pratiques anticoncurrentielles ou d 'un abus de position dominante, ne peut s'apprécier que dans le cadre des relations entre l'exploitant public et la société F.

Que ces pratiques, qu'il appartiendra le cas échéant à la juridiction compétente, déjà saisie, de sanctionner, et le refus de France Télécom d'accéder aux demandes de la société F. tendant à obtenir la communication des données litigieuses selon les modalités autrement définies, ne sauraient en tout état de cause justifier la décision de la société F. de passer outre ce refus, et de contrevenir ainsi aux dispositions légales et réglementaires précitées imposant à tous de respecter le droit d'opposition des tiers à l'utilisation des informations nominatives les concernant à des fins commerciales.

Considérant que l'infraction visée à la prévention apparaît dès lors constituée en tous ses éléments, l'élément intentionnel résultant de la connaissance qu'avaient nécessairement X de la société F. de commercialiser des fichiers dont ils n'avaient pu extraire les noms des abonnés en « liste orange ».

Considérant que l'état de nécessité allégué n'est pas démontré ; qu'il n'est pas justifié d'un péril actuel et imminent ; que la survie de l'entreprise et la sauvegarde de 'emploi invoqués, à les supposer compromis par les décisions de France Télécom, ne peuvent justifier qu'il soit porté atteinte au principe supérieur de la liberté individuelle et de la protection de la vie privée ; qu'au demeurant, la simple affirmation que les coûts pratiqués par France Télécom dans le cadre de ses services Marketis et Teladress sont prohibitifs, alors que d'autres entreprises du même secteur d'activité ont recours à ces services, ne suffit pas à établir l'existence d'une atteinte grave aux intérêts économiques de l'entreprise, « nécessitant un acte de sauvegarde ».

Considérant que l'erreur de droit n'est pas davantage démontrée, les prévenus n'ayant pu se méprendre sur le sens et la portée des textes incriminant l'infraction en cause.

Considérant que le délit de l'article 226-18 du code pénal n'entre pas dans l'énumération des infractions amnistiées en raison de la nature de l'infraction par l'effet de la loi du 3 août 1995.

Considérant que l'article 121-2 du code pénal dispose que « la responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits » ; que le moyen tiré du non cumul de la responsabilité des personnes morales et de celle de leurs représentants légaux doit dès lors être rejeté.

Considérant qu'il y a lieu en conséquence, réformant le jugement entrepris, de déclarer X représentant légal de la société F. et auteur principal des fait visés à la prévention, et cette même société F., pour le compte de laquelle ces faits ont été commis, coupables du délit de l'article 226-18 du code pénal.

Considérant cependant qu'au regard des circonstances particulières de la cause, de la volonté en définitive manifestée par X et la société F. au travers des actions intenses contre France Télécom, de parvenir à concilier la nécessaire protection de la vie privée des personnes avec les règles de la libre concurrence, de leur adhésion à la liste « Stop robinson publicite » mise en place par l'Union française de marketing direct et dont il apparaît d'ailleurs que France Télécom s'est inspirée pour la création de la « liste orange », de faire à leur égard une application modérée de la loi pénale, et de les condamner respectivement à une peine d'amende de 20 000 F et de 100 000 F.

Par ces motifs :

la cour, statuant publiquement et contradictoirement,

En la forme :

- Donne acte à la société F. de ce qu'elle comparaît volontairement sur les faits visés à la prévention ;

- Dit l'appel relevé à titre principal par France Télécom irrecevable ;

— Reçoit l'appel incident du ministère public, et statuant sur les seules dispositions pénales du jugement entrepris :

Au fond :

- Rejette les exceptions soulevées par les intimés ;
- Réforme le jugement déféré en ses dispositions entreprises ;
- Dit X et la société F. coupables du délit visé à la prévention ;
- Condamne X à la peine de 20 000 F d'amende et la société F. à la peine de 100 000 F d'amende ;

Et ont signé le présent arrêt le président et le greffier.

Le greffier,

Le président,

Décision soumise à un droit de procédure (art. 1018 A du code des impôts) : 800 F

L'ARRêT DU CONSEIL D'ÉTAT DU 30 JUILLET 1997

Vu la, requête enregistrée le 12 septembre 1996 au secrétariat du contentieux du Conseil d'État, présentée par la société Consodata dont le siège social est sis 105, rue Jules Guesde à Levallois Perret (92532), représentée par le président du directoire ; la société Consodata demande que le Conseil d'État :

1) annule les délibérations de la Commission nationale de l'informatique et des libertés n° 95-162 et 95-163 du 19 décembre 1995, portant respectivement avertissement et refus de récépissé à la société Consodata ;

2) annule les décisions implicites de rejet de la Commission nationale de l'informatique et des libertés des recours gracieux formés par la société Consodata à l'encontre de ces délibérations ;

3) annule l'absence de délivrance par la Commission nationale de l'informatique et des libertés des récépissés des autres déclarations effectuées par la société Consodata ;

4) ordonne à la Commission nationale de l'informatique et des libertés de publier la décision à intervenir ainsi qu'un rectificatif dans son prochain rapport annuel d'activité, et dans le dossier remis à la presse à l'occasion de la parution de ce prochain rapport ;

Condamne la Commission nationale de l'informatique et des libertés à lui payer la somme de 1 F symbolique, à titre de dommages et intérêts, avec intérêts au taux légal à compter de la décision à intervenir, aux dépens ;

Condamne l'État à lui verser la somme de 10 000 F au titre des frais irrépétibles :

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 le décret n° 65-29 du 11 janvier 1965 ;

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.

Après avoir entendu en audience publique :

- le rapport de M. Pécheur, maître des requêtes ;
- les observations de la SCP Rouvière, Boutet, avocat de la société Consodata ;
- les conclusions de M. Combrexelle, commissaire du Gouvernement.

Sur les conclusions tendant à l'annulation des refus de la Commission nationale de l'informatique et des libertés récépissé des déclarations des traitements de la société Consodata :

En ce qui concerne les conclusions aux fins de non-lieu présentées par la Commission nationale de l'informatique et des libertés :

Considérant que par décisions en date du 18 Février 1997, postérieures à l'introduction du pourvoi, la Commission nationale de l'informatique et des libertés a délivré récépissé, d'une part, des déclarations modificatives du traitement déclaré par la société Consodata le 29 mars 1995, d'autre part, des déclarations de ladite société relatives à la création d'un service « audiotel » et d'un service « minitel » ; qu'ainsi les conclusions susanalysées sont devenues sans objet ; qu'il n'y a plus lieu d'y statuer.

En ce qui concerne les conclusions tendant à l'annulation de l'avertissement en date du 19 décembre 1995 adressé par la Commission nationale de l'informatique et des libertés à la société Consodata :

Sans qu'il soit besoin d'examiner la fin de non-recevoir opposée par la Commission nationale de l'informatique et des libertés :

Considérant, en premier lieu, qu'aux termes de l'article 16 de la loi susvisée du 6 janvier 1978 : « 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 » et qu'aux termes de l'article 19 de la même loi « : » La déclaration doit préciser :... les caractéristiques... du traitement... Toute modification aux mentions énumérées que la société Consodata a fait le 3 février 1995, une déclaration de traitement automatisé de prospects « , constitué à partir de questionnaires comportant, d'une part, plus de 160 questions relatives aux habitudes de consommation des personnes interrogées, d'autre part, une » case à cocher « permettant, en tant que de besoin, à ces personnes de manifester immédiatement leur opposition à ce que les données nominatives les concernant soient cédées à des tiers ; que s'il a été délivré récépissé de cette déclaration le 29 mars 1995, la société Consodata a, dans un second questionnaire, supprimé cette » case à cocher « et l'a remplacée par une mention informant les personnes interrogées qu'elles pouvaient, en écrivant à la société Consodata, s'opposer à la communication à des tiers des informations nominatives les concernant ; que la modification ainsi introduite portant sur une caractéristique essentielle du traitement, la société Consodata était tenue, en vertu des dispositions combinées des articles 16 et 19 précités, de déclarer le nouveau traitement à la Commission nationale de l'informatique et des libertés

Considérant, en second lieu, qu'aux termes de l'article 6 de la loi susvisée la Commission nationale de l'informatique et des libertés « 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 », et qu'aux termes de l'article 26 de la même loi « 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... » ; qu'il ressort des pièces du dossier que la suppression de la case à cocher décidée par la société Consodata avait pour objet et pour effet de réduire le nombre de personnes interrogées par questionnaires manifestant leur opposition à la cession à des tiers des données nominatives les concernant ; que, dans les circonstances de l'espèce, la Commission nationale de l'informatique et des libertés a pu sans commettre d'erreur de droit ni d'erreur d'appréciation estimer que le nouveau traitement ne présentait pas des garanties suffisantes pour permettre aux personnes interrogées d'exercer le droit

d'opposition qui leur est reconnu par l'article 26 précité ; que, par suite, la Commission a pu légalement adresser pour ce motif un avertissement à la Société Consodata.

Sur les conclusions tendant à l'annulation de la décision implicite par laquelle la Commission nationale de l'informatique et des libertés a rejeté le recours gracieux de la société requérante dirigé contre les délibérations n° 95-162 et n° 95-163 :

Considérant qu'en vertu de l'article 1er du décret susvisé du 11 janvier 1*965,* le silence gardé pendant plus de quatre mois sur une réclamation par l'autorité compétente vaut décision de rejet ; qu'il est constant que la société Consodata a présenté à la Commission nationale de l'informatique et des libertés le 15 mars 1996 un recours gracieux dirigé contre les délibérations susmentionnées du 19 décembre 1995 ; que le silence gardé sur cette réclamation pendant plus de quatre mois a fait naître une décision implicite de rejet qui doit être regardée comme émanant de la Commission elle-même : que, dans ces conditions, le moyen tiré de ce que cette décision, faute de délibération de la Commission, sera entachée d'incompétence, ne saura être accueilli.

Sur les conclusions en indemnité présentées par la société Consodata

Considérant qu'aux termes de l'article R 83 du code des tribunaux administratifs et des cours administratives d'appel : « Lorsque tout ou partie des conclusions dont est saisi un tribunal administratif, une cour administrative d'appel ou le Conseil d'État ressorti à la compétence d'une juridiction administrative, le tribunal administratif, la cour administrative d'appel ou le Conseil d'État, selon le cas, est compétent, nonobstant les règles de répartition des compétences entre juridictions administratives, pour rejeter les conclusions entachées d'une irrecevabilité manifeste insusceptible d'être couverte en cours d'instance ou pour constater qu'il n'y a pas lieu de statuer sur tout ou partie des conclusions », que les conclusions tendant à ce que la Commission nationale de l'informatique et des libertés soit condamnée à verser à la société requérante la somme de 1 F à titre de dommages-intérêts sont manifestement irrecevables, faute pour la société Consodata d'avoir lié le contentieux en présentant à la Commission nationale de l'informatique et des libertés une demande préalable à cet effet.

Considérant qu'il résulte de tout ce qui précède que les conclusions susanalysées ne peuvent qu'être rejetées.

Sur les conclusions tendant à ce que le Conseil d'État adresse à la Commission nationale de l'informatique et des libertés l'injonction de publier la décision de celui-ci dans son prochain rapport annuel :

Considérant qu'hormis les cas prévus au 1er alinéa de l'article 6-1 de la loi du 16 juillet 1980 modifiée, il n'appartient pas au juge administratif d'adresser des injonctions à l'administration ; que les conclusions susanalysées ne sont donc pas recevables.

Sur ces conclusions de la Société Consodata tendant à l'application des dispositions de l'article 75-1 de la loi du 10 juillet 1991 :

Considérant qu'il y a lieu, dans les circonstances de l'espèce, de faire application des dispositions de l'article 75-1 de la loi susvisée du 10 juillet 1991 et de condamner l'État à payer à la société Consodata une somme de 5 000 F au titre des frais exposés par elle et non compris dans les dépens.

Décide :

Article 1er : il n'y a pas lieu de statuer sur les conclusions de la requête de la société Consodata dirigées contre les refus de la Commission nationale de l'informatique et des libertés de délivrer récépissé opposés à la société Consodata.

Article 2 : l'État est condamné à payer à la société Consodata la somme de 5 000 F en application de l'article 75-1 de la loi du 10 juillet 1991.

Article 3 : le surplus des conclusions de la requête de société Consodata est rejeté.

Article 4 : la présente décision sera notifiée à la société Consodata, à la Commission nationale de l'informatique et des libertés et au Premier ministre.

L'ARRêT DU CONSEIL D'ÉTAT DU 29 DÉCEMBRE 1997

Vu la requête enregistrée le 11 août 1992 au secrétariat du contentieux du Conseil d'État, présentée pour X ;

M. X demande au Conseil d'État d'annuler pour excès de pouvoir : — la décision notifiée par le président de la Commission nationale de l'informatique et des libertés en date du 19 juin 1992, reprenant plusieurs décisions antérieures notifiées en 1991 et 1992;

- une décision du ministre de la Défense ;
- la lettre du ministre de l'Intérieur en date du 9 janvier 1992 ;
- la décision notifiée par le président de la Commission de contrôle interne de l'organisation internationale de police criminelle Interpol en date du 14 mars 1991 ;
- une décision du ministre des Affaires étrangères.

Vu les autres pièces du dossier ; Vu la loi n° 78-17 du 6 janvier 1978 ; Vu le décret n° 84-172 du 6 mars 1984 ; Vu le décret n° 91-1051 du 14 octobre 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. Après avoir entendu une audience publique :

- le rapport de M^{me} Dayan, conseiller d'État ;
- les observations de la SCP Lesourd, Baudin, avocat de M. X ;
- les conclusions de M^{me} Daussun, commissaire du Gouvernement.

Sur les conclusions dirigées contre de prétendues décisions du ministre de l'Intérieur, du ministre de la Défense et du ministre des Affaires étrangères :

Considérant que la lettre en date du 9 janvier 1992 du ministre de l'Intérieur se borne à un rappel des dispositions relatives à la consultation des fichiers sous sa responsabilité et ne contient aucune décision susceptible de recours pour excès de pouvoir ; que le requérant n'attaque aucune décision du ministre de la Défense expressément désignée ; que la circonstance, alléguée par le requérant, que les ministres successivement charges des Affaires étrangères auraient contribué à la propagation d'informations le concernant contenues dans des fichiers détenus par les autorités françaises, ne constitue pas ni ne révèle une décision susceptible de recours pour excès de pouvoir ; que les conclusions susmentionnées sont frappées d'une irrecevabilité manifeste et non susceptible d'être couverte en cours d'instance.

Sur les conclusions concernant les décisions de la Commission de contrôle interne des fichiers de l'Organisation internationale de police criminelle « Interpol » :

Considérant que l'Organisation internationale de police criminelle « Interpol » n'est pas une autorité administrative française ; que, par suite, les conclusions de M. X tendant à l'annulation des décisions susmentionnées ne sont pas au nombre de celles dont il appartient à la juridiction administrative de connaître.

Sur les conclusions dirigées contre les décisions de la Commission nationale de l'informatique et des libertés :

Considérant qu'aux termes de l'article 39 de la loi du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés : « En ce qui concerne les traitement 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 commission, il est notifié au requérant qu'il a été procédé aux vérifications ».

Considérant que M. X a demandé à la Commission nationale de l'informatique et des libertés l'accès aux informations le concernant qui seraient contenues dans les fichiers des Renseignements généraux, de la direction de la surveillance du territoire, de la direction générale de la sécurité extérieure et de la Gendarmerie.

Considérant que la Commission nationale de l'informatique et des libertés, saisie de ces demandes a, d'une part, fait savoir à M. X, en application du 4° alinéa de l'article 7 du décret du 14 octobre 1991, qu'il n'était fiché ni aux Renseignements généraux, ni à la Gendarmerie nationale, d'autre part, désigné un de ses membres pour procéder aux vérifications des autres fichiers visés par M. X et l'a enfin informé de ce qu'il avait été procédé aux vérifications.

Considérant que l'article 39 précité de la loi du 6 janvier 1978 limite l'accès aux traitements intéressant la sûreté de l'État, la défense et la sécurité publique à un droit d'accès indirect exercé par un membre de la Commission nationale de l'informatique et des libertés ; que les fichiers de la direction de la surveillance du territoire et de la direction générale de la sécurité extérieure sont au nombre des fichiers visés à cet article et ne pouvaient faire l'objet que du droit d'accès indirect prévu par cet article, sans que la Commission nationale de l'informatique et des libertés dispose du droit de donner à l'intéressé communication des informations le concernant, quelles qu'elles soient ; qu'en répondant à M. X qu'il avait été procédé aux vérifications sans lui donner connaissance des constatations faites par son commissaire, non plus que des éventuelles rectifications qu'il aurait apportées aux fichiers en cause, la Commission nationale de l'informatique et des libertés a ainsi fait une exacte application des dispositions de la loi du 6 janvier 1978.

Considérant il est vrai que M. X soutient que l'article 39 précité de la loi du 6 janvier 1978 sur le fondement duquel la Commission nationale de l'informatique et des libertés a traité sa demande serait contraire à l'article 8 de la Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée le 28 janvier 1981 et ratifiée par la France ; que, toutefois, compte tenu des stipulations de l'article 9 de ladite Convention, qui autorisent les États signataires à déroger par la loi aux stipulations de l'article 8 lorsqu'une telle mesure est nécessaire à la protection de la sécurité de l'État ou de la sûreté publique, les modalités d'accès prévues par l'article 39 précité de la loi du 6 janvier 1978 ne sont pas, eu égard à la nature des traitements concernés, incompatibles avec les stipulations conventionnelles susmentionnées.

Considérant qu'il résulte de tout ce qui précède que la requête de M. X doit être rejetée.

Article 1^{sr} : la requête de M. X est rejetée.

Article 2 : la présente décision sera notifiée à M. X, au ministre de l'Intérieur, au ministre de la Défense et au président de la Commission nationale de l'informatique et des libertés

L'ARRET DU CONSEIL D'ETAT DU 28 MARS 1997

Vu, enregistré au secrétariat du Contentieux du Conseil d'État, le 9 octobre 1996, le jugement en date du 29 novembre 1995 par lequel le tribunal administratif de Paris a transmis au Conseil d'État, 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. Henri Solana.

Vu la demande, enregistrée au greffe du tribunal administratif de Paris le 13 août 1992, présentée par Henri Solana et tendant à l'annulation de la décision en date du 22 juin 1992 par laquelle le président de la Commission nationale de l'informatique et des libertés l'a informé que cette Commission avait classé la plainte qu'il lui avait adressée concernant la communication au maire de Saint-Laurent-de-Médoc de la liste des adhérents de l'association Ordinaclub.

Vu les autres pièces du dossier ;

Vu la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales ;

Vu le code civil, et notamment son article 9 ;

Vu le code des communes, et notamment son article L 221-8 ;

Vu la loi du 1er juillet 1901 relative au contrat d'association ;

Vu le décret-loi du 30 octobre 1935 ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu le code des tribunaux administratifs et des cours administratives d'appel ;

Vu le décret n° 53-1169 du 28 novembre 1953 modifié, notamment par le décret n° 72-143 du 22 février 1972 ;

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 ;

Après avoir entendu en audience publique ;

- le rapport de M. Pêcheur, maître des requêtes ;
- les conclusions de M. Combrexelle, Commissaire du Gouvernement.

Sur les fins de non-recevoir opposées par la Commission nationale de l'informatique et des libertés :

Considérant, d'une part, qu'aux termes de l'article 21 de la loi susvisée du 6 janvier 1978 : « Pour l'exercice de sa mission de contrôle, la Commission :... 6 reçoit les réclamations, pétitions et plaintes... » ; que, par lettre en date du 22 juin 1992, le président de la Commission nationale de l'informatique et des libertés a fait connaître à Henri Solana que la Commission avait classé en l'état la plainte que celui-ci lui avait adressée et qui portait sur la communication par le président de l'association Ordinaclub au maire de Saint-Laurent-du-Médoc de la liste des adhérents de cette association ; que le refus de la Commission de donner suite à la plainte déposée auprès d'elle par Henri Solana, fondé sur le motif que l'article 2 du décret-loi du 30 octobre 1935 relatif au contrôle des associations, oeuvres et entreprises subventionnées autorisait une telle communication dès lors qu'aucune copie de la liste des adhérents n'était prise ou conservée, a le caractère d'une décision susceptible de faire l'objet d'un recours pour excès de pouvoir ; que, d'autre part, Henri Solana justifie d'un intérêt lui donnant qualité pour former un tel recours ; que, par suite, les fins de non-recevoir opposées par la Commission nationale de l'informatique et des libertés doivent être écartées.

Sur la légalité de la décision attaquée :

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

Considérant, d'une part, qu'aux termes de l'article L 221-8 du code des communes, en vigueur la date de la décision attaquée : « Toute Association, oeuvre ou entreprise ayant reçu une subvention peut être soumise au contrôle des délégués de la commune qui a accordé cette subvention. Tous groupements, associations, œuvres ou entreprises privées qui ont reçu dans l'année en cours une ou plusieurs subventions sont tenus de fournir à l'autorité qui a mandaté la subvention une copie certifiée de leurs budgets et de leurs comptes de l'exercice écoulé, ainsi que tous documents faisant connaître les résultats de leur activité » ; que la demande du maire de la commune de Saint-Laurent-du-Médoc de prendre connaissance de la liste nominative des adhérents de l'association Ordinaclub, dans le cadre de l'instruction de la demande de renouvellement de la subvention présentée par ladite association, excède les pouvoirs que l'article L. 221-8 précité reconnaît à l'autorité communale d'exiger les documents faisant connaître les résultats de l'activité d'une Association subventionnée.

Considérant, d'autre part, que la communication à l'autorité communale d'une liste nominative des adhérents d'une association, même subordonnée comme en l'espèce à l'interdiction faite à la commune d'en prendre copie, méconnaît le principe de la liberté d'association, lequel a valeur constitutionnelle.

Considérant qu'il résulte de tout ce qui précède que Henri Solana est fondé à demander l'annulation pour excès de pouvoir de la décision par laquelle la Commission nationale de l'informatique et des libertés a classé en l'état sa plainte.

Décide :

Article 1er : la décision en date du 22 juin 1192 de la Commission nationale de l'informatique et des libertés est annulée.

Article 2 : la présente décision sera notifiée à Henri Solana, à la Commission nationale de l'informatique et des libertés et au Premier ministre.

L'ARRÊT DU CONSEIL D'ÉTAT DU 9 JUILLET 1997

Vu, enregistrés au secrétariat du contentieux du Conseil d'État, le 15 juin et le 15 octobre 1993, la requête sommaire et le mémoire complémentaire, présentés pour la chambre syndicale Syntec Conseil, dont le siège est, 3, rue Léon Bonnet, Paris XVIe représentée par son gérant en exercice, domicilié audit siège ; la chambre syndicale Syntec Conseil demande au Conseil d'État d'annuler pour excès de pouvoir la délibération de la Commission nationale de l'informatique et des libertés, qui lui a été notifiée le 15 avril 1993 par le président de la Commission ;

Vu les autres pièces du dossier ;

Vu le code civil ;

Vu la loi n° 77-808 du 19 juillet 1977 relative à la publication et à la diffusion des sondages ;

Vu la loi n° 78-17 du 6 janvier 1978, ensemble le décret n° 78-774 du 17 juillet 1978, modifié par le décret du 4 avril 1991 ;

Vu l'ordonnance n° 45-1708 du 31 juillet 1945, le décret n° 53-934 du 30 septembre 1953 à la loi n° 87-1127 du 31 décembre 1987 ;

Après avoir entendu en audience publique :

— le rapport de M. Gounin, auditeur,
— les observations de la SCP Piwnica, Molinié, avocat de la chambre syndicale Syntec Conseil,
— les conclusions de M. Combrexelle, commissaire du Gouvernement.

Considérant que, par la délibération attaquée, la Commission nationale de l'informatique et des libertés (CNIL) a décidé que, lorsqu'un sondage d'opinion, qui fait

l'objet d'un traitement automatisé, comprend des questions par lesquelles il est demandé aux personnes interrogées ce qu'elles pensent d'une personnalité, celle-ci a, sur le fondement de l'article 34 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un droit d'accès aux informations contenues dans ce sondage, même s'il n'est ni publié, ni diffusé, ainsi qu'un droit à connaître l'identité de la personne ayant commandé la réalisation du sondage ;

Sur les fins de non-recevoir opposées à la requête par la CNIL :

Considérant, d'une part, que la délibération attaquée ne se borne pas à commenter les prescriptions législatives que la CNIL a pour mission de mettre en œuvre, mais qu'elle en fait une interprétation qui ajoute à l'ordonnancement juridique ; que les conclusions tendant à l'annulation de cette délibération sont, par suite, recevables ;

Considérant, d'autre part, que ladite délibération n'étant pas purement confirmative de celle déjà adoptée par la Commission en 1983, les conclusions susanalysées ne sont pas tardives ;

Sur la légalité de la délibération attaquée et sans qu'il soit besoin d'examiner les autres moyens de la requête :

Considérant qu'aux termes de l'article 4 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « 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... », et qu'aux termes de l'article 34 de la même loi, « toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en oeuvre les traitements automatisés dont la liste et 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 » ; qu'enfin les articles 35 et 36 de la loi accordent au titulaire du droit d'accès organisé par l'article 34 un droit de communication de ces informations, ainsi que le droit d'en obtenir, le cas échéant, la rectification ou l'effacement ;

Considérant qu'un sondage, comportant des questions qui demandent aux personnes interrogées ce qu'elles pensent d'une personnalité, ne contient pas des informations qui s'appliquent à celle-ci au sens de l'article 4 précité de la loi du 6 janvier 1978 ; qu'un tel sondage n'a d'autre objet que de chercher à obtenir, par une méthode d'échantillonnage, l'état, à un moment donné, de l'opinion de la population, au sens statistique de ce terme, sur la personnalité qui fait l'objet du sondage ; que, dans ces conditions, il ne résulte ni des dispositions des articles 4 et 34 de la loi, ni d'aucune autre disposition, que les résultats obtenus à partir du dépouillement des réponses aux questions, constitueraient des informations nominatives concernant cette personnalité ; que celle-ci ne saurait, par suite, être titulaire du droit d'accès organisé par l'article 34, ni des droits de communication, de rectification et d'effacement qui en découlent ; qu'elle ne peut, dès lors, ni avoir accès à ce sondage sur le fondement de la loi du 6 janvier 1978, ni exiger de savoir qui a commandé ledit sondage à l'institut qui l'a réalisé ;

Considérant qu'il suit de là que la chambre syndicale Syntec Conseil est fondée à demander l'annulation de la délibération attaquée ;

Décide :

Article 1er : La délibération de la Commission nationale de l'informatique et des libertés, notifiée par son président la chambre syndicale Syntec Conseil le 15 avril 1993, est annulée.

Article 2 : La présente décision sera notifiée à la chambre syndicale Syntec Conseil, à la Commission nationale de l'informatique et des libertés et au garde des Sceaux, ministre de la Justice.

Annexe 8

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

Le Parlement européen et le Conseil de l'Union européenne, vu le traité instituant la Communauté européenne, et notamment son article 100 A, vu la proposition de la Commission , vu l'avis du Comité économique et social ,
statuant conformément à la procédure visée à l'article 189 B du traité , au vu du projet commun approuvé le 6 novembre 1997 par le comité de conciliation,

(1) considérant que la directive 95/46/Œ 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 [4] requiert que les États membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, et notamment le droit au respect de leur vie privée, afin d'assurer la libre circulation des données à caractère personnel dans la Communauté ;

(2) considérant que la confidentialité des communications est garantie en conformité avec les instruments internationaux relatifs aux Droits de l'homme (notamment la convention européenne de sauvegarde des Droits de l'homme et des libertés fonda mentales) et les constitutions des États membres ;

(3) considérant que sont actuellement introduites dans les réseaux publics de télécommunications de la Communauté de nouvelles technologies numériques avancées qui posent des exigences spécifiques concernant la protection des données à caractère personnel et la vie privée des usagers ; que le développement de la société de l'information se caractérise par l'introduction de nouveaux services de télécommunications ; que le succès du développement transfrontalier de ces services, tels que la vidéo à la demande ou la télévision interactive, dépend en partie de la certitude qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée ;

(4) considérant que tel est le cas, en particulier, de l'introduction des réseaux numériques à intégration de services (RNIS) et des réseaux numériques mobiles ;

considérant que, dans sa résolution, du 30 juin 1988, sur le développement du marché commun des services et des équipements des télécommunications d'ici à 1992 [5], le Conseil a préconisé de prendre des mesures pour protéger les données à caractère personnel, afin de créer un environnement adéquat pour le développement futur des télécommunications dans la Communauté ; que le Conseil a derechef souligné l'importance de la protection des données à caractère personnel et de la vie privée dans sa résolution, du 18 juillet 1989, concernant le renforcement de la coordination pour

1 *JO* C 200 du 22 juillet 1994, p. 4.
2 *JO C 159* du 17 juin 1991, p. 38.
3 Avis du Parlement européen du 11 mars 1992 (JO C 94 du 13 avril 1992, p. 198) position commune du Conseil du 12 septembre 1996 *(JO* C 315 du 24 octobre 1996, p. 30) et décision du Parlement européen du 16 janvier 1997 J*O C* 33 du 3 février 1997, p. 78). Décision du Parlement européen du 20 novembre 1997. JO C 371 du 8. décembre 1997). Décision du Conseil du 1" décembre 1997.
4 *JO* L 281 du 23 novembre 1995, p. 31.
5 JO C 257 du 4 octobre 1988, p. 1.

l'introduction du réseau numérique à intégration de services (RNIS) dans la Communauté européenne pour 1992 [1] ;

(6) considérant que le Parlement européen a souligné l'importance de la protection des données à caractère personnel et de la vie privée dans les réseaux de télécommunications, eu égard notamment à l'introduction des réseaux numériques à intégration de services (RNIS) ;

(7) considérant que, dans le cas des réseaux publics de télécommunications, des dispositions législatives, réglementaires et techniques spécifiques doivent être adoptées afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment en ce qui concerne le risque croissant lié au stockage et au traitement automatisés de données relatives aux abonnés et aux utilisateurs ;

(8) considérant que les dispositions législatives, réglementaires et techniques adoptées par les États membres en ce qui concerne la protection des données à caractère personnel, de la vie privée et des intérêts légitimes des personnes morales, dans le secteur des télécommunications, doivent être harmonisées afin d'éviter de créer des obstacles au marché intérieur des télécommunications conformément à l'objectif énoncé à l'article 7 A du traité ; que l'harmonisation est limitée aux exigences qui sont nécessaires pour garantir que la promotion et le développement de nouveaux services et réseaux de télécommuni cations entre États membres ne seront pas entravés ;

(9) considérant que les États membres, les prestataires et les utilisateurs concernés ainsi que les institutions communautaires compétentes devraient coopérer à la conception et au développement des technologies pertinentes requises, en tant que de besoin, pour mettre en œuvre les garanties prévues par la présente directive ;

(10) considérant que ces nouveaux services comprennent la télévision interactive et la vidéo à la demande ;

(11) considérant que, dans le secteur des télécommunications, notamment pour tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels, la directive 95/46/Œ est d'application ; que la directive 95/46/CE s'applique aux services de télécommunications qui ne sont pas accessibles au public ;

(12) considérant que la présente directive, à l'instar de ce que le prévoit l'article 3 de la directive *95/46/Œ,* ne porte pas sur la protection des droits et libertés fondamentaux dans le cas d'activités qui ne sont pas régies par le droit communautaire ; qu'il appartient aux États membres de prendre les mesures qu'ils jugent nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'Etat lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou de l'application du droit pénal ; que la présente directive ne porte pas atteinte à la faculté des États membres de procéder à des interceptions légales des télécommunications dans un des buts énoncés ci-dessus ;

(13) considérant que les abonnés à un service de télécommunications accessible au public peuvent être des personnes physiques ou des personnes morales ; que les dispositions de la présente directive visent à protéger, en complétant la directive *95/46/Œ,* les droits fondamentaux des personnes physiques et en particulier le droit au respect de leur vie privée, ainsi que les intérêts légitimes des personnes morales ; que ces dispositions ne peuvent en aucun cas comporter l'obligation pour les États membres

[1] *JO C* 196 du 1 août! 989, p. 4.

d'étendre l'application de ladite directive 95/46/Œ à la protection des intérêts légitimes des personnes morales ; que cette protection est assurée dans le cadre du droit communautaire et les législations nationales applicables ;

(14) considérant que l'application de certaines exigences relatives à l'indication de l'identification des lignes appelante et connectée et à la limitation de cette indication et au renvoi automatique d'appel vers les lignes d'un abonné connectées à des centraux analogiques ne doit pas être rendue obligatoire dans des cas spécifiques où une telle application s'avérerait techniquement impossible ou exigerait un effort économique disproportionné ; que, en raison de l'importance pour les parties intéressées d'être informées de ces cas, les États membres devraient les communiquer à la Commission ;

(15) considérant que les prestataires de services doivent prendre les mesures appropriées pour assurer la sécurité de leurs services, le cas échéant conjointement avec le fournisseur du réseau, et informer les abonnés des risques particuliers liés à une violation de la sécurité du réseau ; que la sécurité s'apprécie en regard des dispositions de l'article 17 de la directive 95/46/Œ;

(16) considérant que des mesures doivent être prises pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou d'un service de télécommunications accessible au public ; que la législation nationale de certains États membres interdit uniquement l'accès non autorisé intentionnel *aux* communications ;

(17) considérant que les données relatives aux abonnés qui sont traitées pour établir des communications contiennent des informations sur la vie privée des personnes physiques et ont trait au secret de leur correspondance ou concernent les intérêts légitimes de personnes morales ; que ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la prestation du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée ; que tout autre traitement de ces données que le prestataire du service de télécommunications accessible au public pourrait vouloir effectuer pour la commercialisation de ses propres services de télécommunications ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes, fournies par le prestataire du service de télécommunications accessible au public sur la nature des autres traitements qu'il envisage d'effectuer ;

(18) considérant que l'introduction de factures détaillées a amélioré les possibi lités pour l'abonné de vérifier l'exactitude des montants qui lui sont facturés par le prestataire du service ; que, en même temps, elle risque de porter atteinte à la vie privée des utilisateurs des services de télécommunications accessibles au public ; que, par conséquent, pour protéger la vie privée de l'utilisateur, les États membres doivent encourager la mise au point, dans le domaine des services de télécommunications, d'options telles que d'autres formules de paiement permettant l'accès anonyme ou strictement privé aux services de télécommunications accessibles au public, par exemple des télécartes et des facilités de paiement par carte de crédit ; que les États membres peuvent choisir, aux mêmes fins, d'exiger la suppression d'un certain nombre de chiffres des numéros d'appel mentionnés dans les factures détaillées ;

(19) considérant qu'il est nécessaire, en ce qui concerne l'identification de la ligne appelante, de protéger le droit qu'a l'auteur d'un appel d'empêcher l'indication de l'identification de la ligne à partir de laquelle l'appel est effectué, ainsi que le droit de la personne appelée de refuser les appels provenant de lignes non identifiées ; qu'il est justifié, dans des cas spécifiques, d'empêcher la suppression de l'indication de l'identifi cation de la ligne appelante ; que certains abonnés, en particulier les numéros de type « SOS » et autres organisations similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent ; qu'il est nécessaire, en ce qui concerne l'identification de la ligne

connectée, de protéger le droit et l'intérêt légitime qu'a la personne appelée d'empêcher l'indication de l'identification de la ligne à laquelle l'auteur de l'appel est effectivement connecté, en particulier dans le cas d'appels renvoyés ; que les prestataires de services de télécommunications accessibles au public doivent informer leurs abonnés de l'existence, sur le réseau, de l'identification des lignes appelantes et connectées, ainsi que de tous les services offerts sur la base de l'identification des lignes appelantes et connectées et des possibilités offertes en matière de protection de la vie privée ; que cela permettra aux abonnés de choisir en connaissance de cause, parmi les possibilités qui leur sont offertes en matière de protection de la vie privée, celles dont ils souhaiteraient faire usage ; que les possibilités qui sont offertes en matière de protection de la vie privée pour chaque ligne ne doivent pas nécessairement être disponible comme un service automatique du réseau, mais peuvent être obtenues sur simple demande auprès du prestataire du service de télécommunications accessible au public ;

(20) considérant qu'il importe de protéger les abonnés contre toute gêne que pourrait leur causer le renvoi automatique d'appels par d'autres personnes ; que, en pareil cas, les abonnés doivent pouvoir faire cesser le transfert des appels renvoyés sur leurs terminaux sur simple demande adressée au prestataire du service de télécommunications accessible au public ;

(21) considérant que les annuaires sont largement diffusés et accessibles au public ; que, pour protéger la vie privée des personnes physiques et l'intérêt légitime des personnes morales, il importe que l'abonné soit à même de déterminer dans quelle mesure les données à caractère personnel qui le concernent sont publiées dans un annuaire ; que les États membres peuvent limiter cette possibilité aux abonnés qui sont des personnes physiques ;

(22) considérant qu'il importe de protéger les abonnés contre toute violation de leur vie privée par des appels ou des télécopies non sollicités ; que les États membres peuvent limiter cette protection aux abonnés qui sont des personnes physiques ;

(23) considérant qu'il faut veiller à ce que l'introduction de certaines caractéris tiques techniques des équipements de télécommunications en vue d'assurer la protection des données soit harmonisée pour être compatible avec la mise en oeuvre du marché intérieur ;

(24) considérant notamment que, à l'instar de ce que prévoit l'article 13 de la directive 95/46/CE, les États membres peuvent, dans certaines circonstances, limiter la portée des obligations et des droits des abonnés, par exemple en veillant à ce que le prestataire d'un service de télécommunications accessible au public puisse empêcher la suppression de l'indication de l'identification de la ligne appelante, conformément à la législation nationale aux fins de prévenir ou de détecter les infractions pénales ou de sauvegarder la sûreté de l'État ;

(25) considérant que, lorsque les droits des usagers et des abonnés ne sont pas respectés, la législation nationale doit prévoir des recours juridictionnels ; que des sanctions doivent être infligées à toute personne, qu'elle relève du droit privé ou du droit public, qui ne respecte pas les mesures nationales prises en vertu de la présente directive ;

(26) considérant qu'il est utile, dans le champ d'application de la présente directive, d'exploiter l'expérience du groupe « protection des personnes à l'égard du traitement des données à caractère personnel », composé de représentants des autorités de contrôle des États membres, qui a été institué par l'article 29 de la directive 95/46/CE;

(27) considérant que, compte tenu des progrès technologiques et de l'évolution correspondante des services qui sont offerts, il faudra spécifier du point de vue technique les catégories de données figurant à l'annexe de la présente directive aux fins de

l'application de l'article 6 de la présente directive, avec le concours du comité composé de représentants des États membres, institué par l'article 31 de la directive *95/46/Œ,* afin d'assurer une application cohérente des exigences fixées dans la présente directive indépendamment de l'évolution de la technologie ; que cette procédure s'applique exclusivement aux spécifications nécessaires pour adapter l'annexe à de nouveaux progrès technologiques en prenant en considération les changements dans le marché ou dans la demande des consommateurs ; qu'il incombe à la Commission de dûment informer le Parlement européen de son intention d'appliquer cette procédure et que, sinon, la procédure prévue à l'article 100 A s'appliquera ;

(28) considérant que, pour faciliter le respect de la présente directive, certaines dispositions spécifiques sont nécessaires pour le traitement des données déjà commencé à la date d'entrée en vigueur des législations nationales mettant en application la présente directive,

Ont arrêté la présente directive :

Article premier : objet et champ d'application

1) La présente directive concerne l'harmonisation des dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des télécommunications, ainsi que la libre circulation de ces données et des équipements et services de télécommunications dans la Communauté.

2) Les dispositions de la présente directive précisent et complètent la directive *95/46/Œ* aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3) La présente directive ne s'applique pas aux activités qui ne relèvent pas du droit communautaire, telles que celles visées aux titres V et VI du traité sur l'Union européenne ni, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.

Article 2 : définitions

Outre les définitions figurant dans la directive *95/46/Œ,* aux fins de la présente directive, on entend par :

a) « abonné » : toute personne physique ou morale qui a conclu un contrat avec le prestataire de services de télécommunications accessibles au public en vue de la fourniture de tels services ;

b) « utilisateur » : toute personne physique utilisant un service de télécommunications accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

c) « réseau public de télécommunications » : les systèmes de transmission et, le cas échéant, l'équipement de commutation et les autres ressources permettant le transport de signaux entre des points de terminaison définis, par fils, par faisceaux hertziens, par moyens optiques ou par d'autres moyens électromagnétiques, qui sont utilisés, en tout ou en partie, pour la fourniture de services télécommunications accessibles au public ;

d) « service de télécommunications » : les services qui consistent, en tout ou en partie, en la transmission et l'acheminement de signaux sur des réseaux de télécommunications, à l'exception de la radiodiffusion et de la télévision.

Article 3 : services concernés

1) La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications accessibles au public sur les réseaux publics de télécommunications dans la Communauté, notamment via le réseau numérique à intégration de services (RNIS) et les réseaux numériques mobiles publics.

2) Les articles 8, 9 et 10 s'appliquent aux lignes d'abonnés connectées à des centraux numériques et, lorsque cela est techniquement possible et ne nécessite pas un effort économique disproportionné, aux lignes d'abonnés connectées à des centraux analogiques.

3) Lorsqu'il est techniquement impossible de se conformer aux exigences des articles 8, 9 et 10 ou lorsque cela nécessite un investissement disproportionné, les États membres en informent la Commission.

Article 4 : sécurité

1) Le prestataire d'un service de télécommunications accessible au public doit prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de télécommunications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en oeuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.

2) Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le prestataire d'un service de télécommunications accessible au public doit informer les abonnés de ce risque ainsi que de tout moyen éventuel d'y remédier, y compris le coût que cela implique.

Article 5 : confidentialité des communications

1) Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommu nications ou de services de télécommunications accessibles au public. En particulier, ils interdisent à toute 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.

2) Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications, dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

Article 6 : données relatives au trafic et à la facturation

1) Les données relatives au trafic concernant les abonnés et les utilisateurs traitées en vue d'établir des communications et stockées par le fournisseur d'un réseau public de télécommunications et/ou d'un service de télécommunications accessible au public doivent être effacées ou rendues anonymes dès que la communication est terminée, sans préjudice des dispositions des paragraphes 2, 3 et 4.

2) Dans le but d'établir les factures des abonnés et aux fins des paiements pour interconnexion, les données énumérées à l'annexe peuvent être traitées. 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.

Dans le but de commercialiser ses propres services de télécommunications, le prestataire d'un service de télécommunications accessible au public peut traiter les données visées au paragraphe 2, pour autant que l'abonné ait donné son consentement.

3) Le traitement des données relatives au trafic et à la facturation doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de télécommu nications et/ou de services de télécommunications accessibles au public chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de télécommunications du prestataire ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

4) Les paragraphes 1, 2, 3 et 4 s'appliquent sans préjudice de la possibilité qu'ont les autorités compétentes de se faire communiquer des données relatives à la facturation ou au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.

Article 7 : facturation détaillée

1) Les abonnés ont le droit de recevoir des factures non détaillées.

2) Les États membres appliquent des dispositions nationales afin de concilier les droits des abonnés recevant des factures détaillées avec le droit à la vie privée des utilisateurs appelants et des abonnés appelés, par exemple en veillant à ce que lesdits utilisateurs et abonnés disposent d'autres modalités suffisantes de communication ou de paiement.

Article 8 : indication de l'identification des lignes appelantes et connectées et limitation de cette possibilité

1) Dans les cas où l'indication de l'identification de la ligne appelante est offerte, l'utilisateur appelant doit pouvoir éliminer, par un moyen simple et gratuit, l'indication de l'identification de la ligne appelante, et ce, appel par appel. L'abonné appelant doit avoir cette possibilité pour chaque ligne.

2) Dans les cas où l'indication de l'identification de la ligne appelante est offerte, l'abonné appelé doit pouvoir empêcher, par un moyen simple, gratuit pour un usage raisonnable de cette fonction, l'indication de l'identification de la ligne pour les appels entrants.

3) Dans les cas où l'indication de l'identification de la ligne appelante est offerte et où l'identification de la ligne appelante est indiquée avant l'établissement de l'appel, l'abonné appelé doit pouvoir, par un moyen simple, refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a supprimé l'indication de l'identification de la ligne appelante.

4} Dans les cas où l'indication de l'identification de la ligne connectée est offerte, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, supprimer l'indication de l'identification de la ligne connectée auprès de la personne qui appelle.

5) Les dispositions du paragraphe 1 s'appliquent également aux appels à destination de pays tiers émanant de la Communauté ; les dispositions des paragraphes 2, 3 et 4 s'appliquent également aux appels entrants émanant de pays tiers.

6) Les États membres veillent à ce que, dans les cas où l'indication de l'identification de la ligne appelante et/ou de la ligne connectée est offerte, les prestataires de services de télécommunications accessibles au public informent celui-ci de cette situation, ainsi que des possibilités prévues aux paragraphes 1, 2, 3 et 4.

Article 9 : dérogations

Les États membres veillent à l'existence de procédures transparentes régissant les modalités grâce auxquelles un fournisseur d'un réseau public de télécommunications et/ou d'un service de télécommunications accessible au public peut passer outre à la suppression de l'indication de l'identification de la ligne appelante :

a) à titre temporaire, lorsqu'un abonné demande l'identification d'appels malveillants ou dérangeants ; dans ce cas, conformément au droit interne, les données permettant d'identifier l'abonné appelant seront conservées et communiquées par le fournisseur d'un réseau public de télécommunications et/ou d'un service de télécommunications accessible au public ;

b) ligne par ligne pour les organismes répondant à des appels d'urgence et reconnus comme tels par un État membre, y compris les services de police, les services d'ambulances et les pompiers, dans le but de répondre à de tels appels.

Article 10 : renvois automatiques d'appels

Les États membres veillent à ce que tout abonné ait la possibilité, gratuitement et par un moyen simple, de mettre fin au renvoi automatique des appels par un tiers vers son terminal.

Article 11 : annuaires d'abonnés

1) Les données à caractère personnel figurant dans les annuaires d'abonnés, imprimés ou électroniques, et qui sont à la disposition du public ou que l'on peut obtenir auprès des services de renseignements concernant l'annuaire, doivent être limitées à ce qui est nécessaire pour identifier un abonné particulier, à moins que l'abonné n'ait donné son consentement, sans la moindre ambiguïté, à ce que des données supplémentaires le concernant soient publiées. L'abonné doit avoir le droit d'obtenir gratuitement, sur demande, de ne pas figurer dans un annuaire, imprimé ou électronique, d'indiquer que les données le concernant ne peuvent pas être utilisées à des fins de prospection directe, que son adresse ne figure que partiellement dans l'annuaire et qu'aucune mention relative à son sexe n'y figure, lorsque cela se justifie du point de vue linguistique.

2) Nonobstant le paragraphe 1, les États membres peuvent permettre aux opérateurs d'exiger d'un abonné un paiement afin que ses coordonnées ne figurent pas dans un annuaire, à condition que la somme demandée ne soit pas dissuasive pour l'exercice de ce droit, et que, tout en prenant en compte les exigences de qualité de l'annuaire public au regard du service universel, cette somme soit calculée pour couvrir les coûts effectivement encourus par l'opérateur pour l'adaptation et la mise à jour de la liste des abonnés à ne pas faire figurer dans l'annuaire public.

3) Les droits conférés par le paragraphe 1 s'appliquent aux abonnés qui sont des personnes physiques. Les États membres garantissent également, dans le cadre du droit communautaire et des législations nationales applicables, que les intérêts légitimes des abonnés autres que les personnes physiques sont suffisamment protégés en ce qui concerne leur inscription dans les annuaires publics.

Article 12 : appels non sollicités

1) L'utilisation de systèmes automatisés d'appels sans intervention humaine (automates d'appel) ou de télécopieurs (fax) à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable.

2) Les États membres prennent les mesures appropriées pour faire en sorte que, sans frais pour l'abonné, les appels non sollicités par celui-ci et effectués à des fins de

prospection directe par d'autres moyens que ceux visés au paragraphe 1 ne soient pas autorisés, soit sans le consentement des abonnés concernés, soit à l'égard des abonnés qui ne souhaitent pas recevoir ces appels, le choix entre ces deux solutions étant régi par la législation nationale.

3) Les droits conférés par les paragraphes 1 et 2 s'appliquent aux abonnés qui sont des personnes physiques. Les États membres garantissent également, dans le cadre du droit communautaire et des législations nationales applicables, que les intérêts légitimes des abonnés autres que les personnes physiques sont suffisamment protégés en ce qui concerne les appels non sollicités.

Article 13 : caractéristiques techniques et normalisation

1) Lors de la mise en oeuvre des dispositions de la présente directive, les États membres veillent, sous réserve des paragraphes 2 et 3, à ce qu'aucune exigence obligatoire relative à des caractéristiques techniques spécifiques ne soit imposée aux terminaux ou à d'autres équipements de télécommunications qui pourrait entraver la mise sur le marché d'équipements ou la libre circulation de ces équipements dans les États membres et entre ces derniers.

2) Lorsque des dispositions de la présente directive ne peuvent être mises en œuvre que par le recours à des caractéristiques techniques spécifiques, les États membres en informent la Commission, conformément aux procédures prévues par la directive 83/189/CEE [1], qui instaure une procédure d'information dans le domaine des normes et réglementations techniques.

3) Le cas échéant, la Commission assure l'élaboration de normes européennes communes pour la mise en œuvre de caractéristiques techniques spéciales, conformément aux dispositions du droit communautaire concernant le rapprochement des législations des États membres relatives aux équipements terminaux de télécommunications, y compris la reconnaissance mutuelle de leur conformité, et à la décision 87/95/CEE du Conseil, du 22 décembre 1986, relative à la normalisation dans le domaine des technologies de l'information et des télécommunications [2].

Article 14 : extension du champ d'application de certaines dispositions de la directive 95/46/CE

1) Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 5 et 6 et à l'article 8 paragraphes 1 à 4 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de télécommunications, comme le prévoit l'article 13 paragraphe 1 de la directive 95/46/CE.

2) Les dispositions du chapitre III de la directive 95/46/CE, relatif aux recours juridictionnels, à la responsabilité et aux sanctions, sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3) Le groupe « protection des personnes à l'égard du traitement des données à caractère personnel » institué par l'article 29 de la directive 95/46/CE remplit les tâches visées à l'article 30 de ladite directive également en ce qui concerne la protection des

1 *JO C* 196 du 1 août 1989, p. 4.
2 *JO* L 36 du 7 février 1987, p. 31. Décision modifiée en dernier lieu par l'acte d'adhésion de 1994.

droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des télécommunications, qui est l'objet de la présente directive.

Article 15 : mise en oeuvre de la directive

1) Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 24 octobre 1998. Par dérogation au premier alinéa, les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à l'article 5 de la présente directive au plus tard le 24 octobre 2000. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence, lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2) Par dérogation à l'article 6 paragraphe 3, le consentement n'est pas requis s'il s'agit d'un traitement déjà commencé à la date d'entrée en vigueur des dispositions nationales adoptées en application de la présente directive. En pareil cas, les abonnés sont informés de ce traitement et, s'ils ne s'y sont pas opposés dans un délai à fixer par les États membres, sont réputés avoir donné leur consentement.

3) L'article 11 ne s'applique pas aux éditions d'annuaires publiées avant l'entrée en vigueur des dispositions nationales adoptées en application de la présente directive.

4) Les États membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 16 : destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 15 décembre 1997. Par le

Parlement européen

Le président J. M. Gil-Robles

Par le Conseil

Le président J. C.Juncker

Annexe : liste des données

Aux fins de l'article 6 paragraphe 2, peuvent être traitées les données visées ci-après indiquant :

- le numéro ou le poste de l'abonné ;
- l'adresse de l'abonné et le type de poste ;
- le nombre total d'unités à facturer pour la période de facturation ;
- le numéro de l'abonné appelé ;
- le type d'appels, l'heure à laquelle ils ont commencé et la durée des appels effectués et/ou la quantité de données transmises ;
- la date de l'appel ou du service ;

.— d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.

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

Le Parlement européen et le Conseil de l'Union européenne, vu le traité instituant la Communauté européenne, et notamment son article 100 A, vu la proposition de la Commission [1],
vu l'avis du Comité économique et social [2], statuant conformément à la procédure prévue à l'article 189 B du traité[3], au vu du projet commun approuvé le 27 novembre 1996 par le comité de conciliation,

(1) considérant qu'il importe, dans le cadre de la réalisation des objectifs du marché intérieur, d'arrêter les mesures destinées à consolider progressivement ce marché ;

(2) considérant que la libre circulation des biens et des services concerne non seulement le commerce professionnel mais également les particuliers ; qu'elle implique, pour les consommateurs, de pouvoir accéder aux biens et aux services d'un autre Etat membre dans les mêmes conditions que la population de cet État ;

(3) considérant que la vente transfrontalière à distance peut être l'une des principales manifestations concrètes pour les consommateurs de l'achèvement du marché intérieur, comme cela a été constaté, entre autres, dans la communication de la Commission au Conseil intitulée « Vers un marché unique de la distribution » ; qu'il est indispensable, pour le bon fonctionnement du marché intérieur, que les consommateurs puissent s'adresser à une entreprise en dehors de leur pays, même si cette dernière dispose d'une filiale dans le pays de résidence du consommateur ;

(4) considérant que l'introduction de nouvelles technologies entraîne une multi plication des moyens mis à la disposition des consommateurs pour connaître les offres faites partout dans la Communauté et pour passer leurs commandes ; que certains États membres ont déjà pris des dispositions différentes ou divergentes de protection des consommateurs en matière de vente à distance, avec des incidences négatives sur la concurrence entre les entreprises dans le marché intérieur ; qu'il est par conséquent nécessaire d'introduire un minimum de règles communes au niveau communautaire dans ce domaine ;

(5) considérant que les points 18 et 19 de l'annexe de la résolution du Conseil, du 14 avril 1975, concernant un programme préliminaire de la Communauté économique européenne pour une politique de protection et d'information des consommateurs [4] font ressortir la nécessité de protéger les acheteurs de biens ou de services contre la demande de paiement de marchandises non commandées et les méthodes de vente agressives ;

(6) considérant que la communication de la Commission au Conseil intitulée « Nouvelle impulsion pour la politique de protection des consommateurs », qui a été approuvée par la résolution du Conseil du 23 juin 1986 [5], annonce, au point 33, que la Commission présentera des propositions concernant l'utilisation de nouvelles technologies

1 JO n° C 156 du 23 juin 1992, p. 14.

2 *JO* n° C 19 du 25 janvier 1993, p. 111.

3 Avis du Parlement européen du 26 mai 1993 JO n° C 176 du 28 juin 1993, p. 95), position commune du Conseil du 29 juin 1995 (./O n° C 288 du 30 octobre 1995, p. 1) et décision du Parlement européen du 13 décembre 1995 (J*O n°* C 17 du 22. janvier 1996, p. 51). Décision du Parlement européen du 16 janvier 1997 et décision du Conseil du 20 janvier 1997.

4 *JO* n° C 92 du 25 avril 1975, p. 1.

5 *JO* n° C 167 du 5 juillet 1986, p. 1.

de l'information qui permettent aux consommateurs de passer, depuis leur domicile, des commandes à un fournisseur ;

(7) considérant que la résolution du Conseil, du 9 novembre 1989, sur les priorités futures pour la relance de la politique de protection des consommateurs [1] invite la Commission à consacrer ses efforts en priorité aux domaines visés à l'annexe de ladite résolution ; que cette annexe mentionne les nouvelles technologies permettant la vente à distance ; que la Commission a donné suite à cette résolution par l'adoption d'un « plan d'action triennal pour la politique de protection des consommateurs dans la Communauté économique européenne (1990-1992) » et que ce plan prévoit l'adoption d'une directive en la matière ;

(8) considérant que l'emploi des langues en matière de contrats à distance relève de la compétence des États membres ;

(9) considérant que le contrat à distance se caractérise par l'utilisation d'une ou de plusieurs techniques de communication à distance ; que ces différentes techniques sont utilisées dans le cadre d'un système organisé de vente ou de prestation de services à distance sans qu'il y ait présence simultanée du fournisseur et du consommateur ; que l'évolution permanente de ces techniques ne permet pas d'en dresser une liste exhaustive mais nécessite de définir des principes valables même pour celles qui ne sont encore que peu utilisées ;

(10) considérant qu'une même transaction comportant des opérations succes sives ou une série d'opérations distinctes à exécution échelonnée peut donner lieu à des descriptions juridiques différentes selon le droit des États membres ; que les dispositions de la présente directive ne peuvent être appliquées différemment selon le droit des États membres, sous réserve de leur recours à l'article 14 ; que, à cette fin, il y a lieu de considérer qu'il doit y avoir au moins conformité avec les dispositions de la présente directive à la date de la première d'une série d'opérations successives ou de la première d'une série d'opérations distinctes à exécution échelonnée pouvant être considérées comme formant un tout, indépendamment du fait que cette opération ou cette série d'opérations fasse l'objet d'un seul contrat ou de plusieurs contrats successifs distincts ;

(11) considérant que l'utilisation de techniques de communication à distance ne doit pas conduire à une diminution de l'information fournie au consommateur ; qu'il convient donc de déterminer les informations qui doivent être obligatoirement transmises au consommateur, quelle que soit la technique de communication utilisée ; que l'informa tion transmise doit en outre être faite en conformité avec les autres règles communautaires pertinentes, et en particulier avec celles de la directive 84/450/CEE du Conseil, du 10 septembre 1984, relative au rapprochement des dispositions législatives, réglemen taires et administratives des États membres en matière de publicité trompeuse [2] ; que, si des exceptions sont apportées à l'obligation de fournir des informations, il appartient au consommateur, de façon discrétionnaire, de demander certaines informations de base telles que l'identité du fournisseur, les caractéristiques essentielles des marchandises ou des services et leurs prix ;

(12) considérant que, dans le cas d'une communication par téléphone, il convient que le consommateur reçoive suffisamment d'informations au début de la conversation afin de décider s'il continue ou non celle-ci ;

(13) considérant que l'information diffusée par certaines technologies électroni ques a souvent un caractère éphémère dans la mesure où elle n'est pas reçue sur un

1 *JO* n° C 294 du 22 novembre 1989, p. 1.
2 *JO* n° L 250 du 19 septembre 1984, p. 17.

support durable ; qu'il est nécessaire que le consommateur reçoive par écrit, en temps utile, des informations nécessaires à la bonne exécution du contrat ;

(14) considérant que le consommateur n'a pas la possibilité *in concreto* de voir le produit ou de prendre connaissance des caractéristiques du service avant la conclusion du contrat ; qu'il convient de prévoir un droit de rétractation, sauf disposition contraire dans la présente directive ; que, pour que ce droit ne reste pas de pure forme, les éventuels frais supportés par le consommateur lorsqu'il exerce son droit de rétractation doivent être limités aux frais directs de renvoi des marchandises ; que ce droit de rétractation ne doit pas préjuger de l'application des droits dont le consommateur bénéficie en vertu de sa législation nationale, notamment en ce qui concerne la réception de produits endomma gés, de services défectueux ou de produits ou services qui, ne correspondent pas à la description qui en est faite dans l'offre ; qu'il appartient aux États membres de déterminer les autres conditions et modalités consécutives à l'exercice du droit de rétractation ;

(15) considérant qu'il est également nécessaire de prévoir un délai d'exécution du contrat si celui-ci n'a pas été défini lors de la commande ;

(16) considérant que la technique promotionnelle consistant à envoyer un produit ou à fournir un service à titre onéreux au consommateur sans demande préalable ou accord explicite de sa part, pour autant qu'il ne s'agisse pas d'une fourniture de remplacement, ne peut être admise ;

(17) considérant les principes établis par les articles 8 et 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 ; qu'il y a lieu de reconnaître au consommateur un droit à la protection de la vie privée, notamment en ce qui concerne la tranquillité à l'égard de certaines techniques de communication particulièrement envahissantes ; que, en conséquence, il y a lieu de préciser les limites spécifiques à l'usage de pareilles techniques ; que les États membres devraient prendre les mesures nécessaires pour protéger efficacement contre le démarchage les consommateurs qui auront fait savoir qu'ils ne souhaitent pas être démarchés par certains moyens de communication, sans préjudice des sauvegardes particulières dont dispose le consommateur dans le cadre de la législation communautaire relative à la protection des données personnelles et de la vie privée ;

(18) considérant qu'il est important que les règles de base contraignantes contenues dans la présente directive soient complétées, le cas échéant, par des disposi tions volontaires des professionnels concernés, conformément à la recommandation 92/295/CEE de la Commission, du 7 avril 1992, concernant des codes de conduite pour la protection des consommateurs en matière de contrats négociés à distance [1] ;

(19) considérant qu'il est important, dans l'intérêt d'une protection optimale du consommateur, que celui-ci soit informé de façon satisfaisante sur les dispositions de la présente directive ainsi que sur les codes de pratique qui peuvent exister dans ce domaine ;

(20) considérant que le non-respect des dispositions de la présente directive peut porter préjudice aux consommateurs mais aussi aux concurrents ; que l'on peut donc prévoir des dispositions permettant à des organismes publics ou à leur représentant, ou à des organisations de consommateurs ayant, selon la législation nationale, un intérêt légitime à protéger les consommateurs, ou à des organisations professionnelles ayant un intérêt légitime à agir, de veiller à son application ;

(21) considérant qu'il est important pour la protection des consommateurs de traiter, dès que possible, la question des plaintes transfrontalières ; que la Commission a

[1] JO n° L 156 du 10 juin 1992, p. 21.

publié, le 14 février 1996, un plan d'action sur l'accès des consommateurs à la justice et le règlement des litiges de consommation dans le marché intérieur ; que ce plan comporte des initiatives spécifiques visant à promouvoir les procédures extrajudiciaires ; que des critères objectifs (annexe II) sont établis pour garantir la fiabilité de ces procédures et qu'il est prévu d'utiliser des formules de plainte standardisées (annexe III) ;

(22) considérant que, dans l'utilisation des nouvelles technologies, le consomma teur n'a pas la maîtrise de la technique ; qu'il est donc nécessaire de prévoir que la charge de la preuve peut incomber au fournisseur ;

(23) considérant qu'il existe le risque, dans certains cas, de priver le consomma teur de la protection accordée par la présente directive en désignant le droit d'un pays tiers comme droit applicable au contrat ; que, en conséquence, il convient de prévoir dans la présente directive des dispositions visant à éviter ce risque ;

(24) considérant qu'un État membre peut interdire, pour des raisons d'intérêt général, la commercialisation de certains produits et services sur son territoire par voie de contrat à distance ; que cette interdiction doit se faire dans le respect des règles communautaires ; que de telles interdictions sont déjà prévues, notamment en matière de médicaments par la directive 89/552/CEE du Conseil, du 3 octobre 1989, visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à l'exercice d'activités de radiodiffusion télévisuelle [1] et par la directive 92/28/ŒE du Conseil, du 31 mars 1992, concernant la publicité faite à l'égard des médicaments à usage humain [2],

Ont arrêté la présente directive :

Article premier : objet

La présente directive a pour objet de rapprocher les dispositions législatives, réglementaires et administratives des États membres concernant les contrats à distance entre consommateur et fournisseur.

Article 2 : définitions

Aux fins de la présente directive, on entend par :

1) « contrat à distance » : tout contrat concernant des biens ou services conclu entre un fournisseur et un consommateur dans le cadre d'un système de vente ou de prestations de services à distance organisé par le fournisseur, qui, pour ce contrat, utilise exclusivement une ou plusieurs techniques de communication à distance jusqu'à la conclusion du contrat, y compris la conclusion du contrat elle-même ;

2) « consommateur » : toute personne physique qui, dans les contrats relevant de la présente directive, agit à des fins qui n'entrent pas dans le cadre de son activité professionnelle ;

3) « fournisseur » : toute personne physique ou morale qui, dans les contrats relevant de la présente directive, agit dans le cadre de son activité professionnelle ;

4) « technique de communication à distance » : tout moyen qui, sans présence physique et simultanée du fournisseur et du consommateur, peut être utilisé pour la conclusion du contrat entre ces parties. Une liste indicative des techniques visées par la présente directive figure à l'annexe I ;

1 *JO* n° L 298 du 17 octobre 1989, p. 23.
2 *JO* n° L 113 du 30 avril 1992, p. 13.

5) « opérateur de technique de communication » : toute personne physique ou morale, publique ou privée, dont l'activité professionnelle consiste à mettre à la disposition des fournisseurs une ou plusieurs techniques de communication à distance.

Article 3 : exemptions

1) La présente directive ne s'applique pas aux contrats :
— portant sur les services financiers dont une liste non exhaustive figure à l'annexe II,
— conclus par le moyen de distributeurs automatiques ou de locaux commerciaux automatisés ;
— conclus avec les opérateurs de télécommunications du fait de l'utilisation des cabines téléphoniques publiques ;
— conclus pour la construction et la vente des biens immobiliers ou portent sur d'autres droits relatifs à des biens immobiliers, à l'exception de la location ;
— conclus lors d'une vente aux enchères.

2) Les articles 4, 5, 6 et l'article 7 paragraphe 1 ne s'appliquent pas :
— aux contrats de fourniture de denrées alimentaires, de boissons ou d'autres biens ménagers de consommation courante fournis au domicile d'un consommateur, à sa résidence ou à son lieu de travail par des distributeurs effectuant des tournées fréquentes et régulières ;
— aux contrats de fourniture de services d'hébergement, de transports, de restauration, de loisirs, lorsque le fournisseur s'engage, lors de la conclusion du contrat, à fournir ces prestations à une date déterminée ou à une période spécifiée ; exceptionnellement, dans le cas d'activités de loisirs en plein air, le fournisseur peut se réserver le droit de ne pas appliquer l'article 7 paragraphe 2 dans des circonstances spécifiques.

Article 4 : informations préalables

1) En temps utile avant la conclusion de tout contrat à distance, le consommateur doit bénéficier des informations suivantes :
a) identité du fournisseur et, dans le cas de contrats nécessitant un paiement anticipé, son adresse ;
b) caractéristiques essentielles du bien ou du service ;
c) prix du bien ou du service, toutes taxes comprises ;
d) frais de livraison, le cas échéant ;
e) modalités de paiement, de livraison ou d'exécution ;
f) existence d'un droit de rétractation, sauf dans les cas visés à l'article 6 paragraphe 3 ;
g) coût de l'utilisation de la technique de communication à distance, lorsqu'il est calculé sur une base autre que le tarif de base ;
h) durée de validité de l'offre ou du prix ;
i) le cas échéant, durée minimale du contrat dans le cas de contrats portent sur la fourniture durable ou périodique d'un bien ou d'un service.

2) Les informations visées au paragraphe 1, dont le but commercial doit apparaître sans équivoque, doivent être fournies de manière claire et compréhensible par tout moyen adapté à la technique de communication à distance utilisée, dans le respect, notamment, des principes de loyauté en matière de transactions commerciales et des principes qui régissent la protection des personnes frappées d'incapacité juridique selon leur législation nationale, telles que les mineurs.

3) En outre, dans le cas de communications téléphoniques, le fournisseur indique explicitement au début de toute conversation avec le consommateur son identité et le but commercial de l'appel.

Article 5 : confirmation écrite des informations

1) Le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès, confirmation des informations mentionnées à l'article 4 paragraphe 1 points a) à f), en temps utile lors de l'exécution du contrat et au plus tard au moment de la livraison en ce qui concerne les biens non destinés à la livraison à des tiers, à moins que ces informations n'aient déjà été fournies au consommateur préalablement à la conclusion du contrat par écrit ou sur un autre support durable à sa disposition et auquel il a accès.

En tout état de cause, doivent être fournies :
- une information écrite sur les conditions et les modalités d'exercice du droit de rétractation au sens de l'article 6, y compris les cas visés à l'article 6 paragraphe 3 premier tiret ;
- l'adresse géographique de l'établissement du fournisseur où le consommateur peut présenter ses réclamations ;
- les informations relatives aux services après-vente et aux garanties commerciales existants ;
- les conditions de résiliation du contrat lorsque celui-ci est à durée indéterminée ou d'une durée supérieure à un an.

2) Le paragraphe 1 ne s'applique pas aux services dont l'exécution elle-même est réalisée au moyen d'une technique de communication à distance, lorsque ces services sont fournis en une seule fois, et dont la facturation est effectuée par l'opérateur de la technique de communication. Néanmoins, le consommateur doit en tout cas pouvoir avoir connaissance de l'adresse géographique de l'établissement du fournisseur où le consommateur peut présenter ses réclamations.

Article 6 : droit de rétractation

1) Pour tout contrat à distance, le consommateur dispose d'un délai d'au moins sept jours ouvrables pour se rétracter sans pénalités et sans indication du motif. Les seuls frais qui peuvent être imputés au consommateur en raison de l'exercice de son droit de rétractation sont les frais directs de renvoi des marchandises.

Pour l'exercice de ce droit, le délai court :
- pour les biens, à compter du jour de leur réception par le consommateur lorsque les obligations visées à l'article 5 ont été remplies ;
- pour les services, à compter du jour de la conclusion du contrat ou à partir du jour où les obligations prévues à l'article 5 ont été remplies si elles sont remplies après la conclusion du contrat, à condition que le délai n'excède pas le délai de trois mois indiqué à l'alinéa suivant.

Au cas où le fournisseur n'a pas rempli les obligations visées à l'article 5, le délai est de trois mois. Ce délai court :
- pour les biens, à compter du jour de leur réception par le consommateur ;
- pour les services, à compter du jour de la conclusion du contrat.

Si, dans ce délai de trois mois, les informations visées à l'article 5 sont fournies, le délai de sept jours ouvrables indiqué au premier alinéa commence à courir dès ce moment.

2) Lorsque le droit de rétractation est exercé par le consommateur conformément au présent article, le fournisseur est tenu au remboursement des sommes versées par le consommateur, sans frais. Les seuls frais qui peuvent être imputés au consommateur en raison de l'exercice de son droit de rétractation sont les frais directs de renvoi des

marchandises. Ce remboursement doit être effectué dans les meilleurs délais et, en tout cas, dans les trente jours.

3) Sauf si les parties en ont convenu autrement, le consommateur ne peut exercer le droit de rétractation prévu au paragraphe 1 pour les contrats :
- de fourniture de services dont l'exécution a commencé, avec l'accord du consomma teur, avant la fin du délai de sept jours ouvrables prévu au paragraphe 1 ;
- de fourniture de biens ou de services dont le prix est fonction de fluctuations des faux du marché financier, que le fournisseur n'est pas en état de contrôler ;
- de fourniture de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés ou qui, du fait de leur nature, ne peuvent être réexpédiés ou sont susceptibles de se détériorer ou de se périmer rapidement ;
- de fourniture d'enregistrements audio ou vidéo ou de logiciels informatiques descellés par le consommateur ;
- de fourniture de journaux, de périodiques et de magazines ;
- de services de paris et de loteries.

4) Les États membres prévoient dans leur législation que :
- si le prix d'un bien ou d'un service est entièrement ou partiellement couvert par un crédit accordé par le fournisseur ou ;
- si ce prix est entièrement ou partiellement couvert par un crédit accordé au consom mateur par un tiers sur la base d'un accord conclu entre le tiers et le fournisseur, le contrat de crédit est résilié, sans pénalité, lorsque le consommateur exerce son droit de rétractation conformément au paragraphe 1.

Les États membres déterminent les modalités de la résiliation du contrat de crédit.

Article 7 : exécution

1) Sauf si les parties en ont convenu autrement, le fournisseur doit exécuter la commande au plus tard dans un délai de trente jours à compter du jour suivant celui où le consommateur a transmis sa commande au fournisseur.

2) En cas de défaut d'exécution du contrat par un fournisseur résultant de l'indisponibilité du bien ou du service commandé, le consommateur doit être informé de cette indisponibilité et doit pouvoir être remboursé dans les meilleurs délais et, en tout cas, dans les trente jours, des sommes qu'il a, le cas échéant, versées en paiement.

3) Néanmoins, les États membres peuvent prévoir que le fournisseur peut fournir au consommateur un bien ou un service d'une qualité et d'un prix équivalents si la possibilité en a été prévue préalablement à la conclusion du contrat, ou dans le contrat. Le consommateur est informé de cette possibilité de manière claire et compréhensible. Les frais de retour consécutifs à l'exercice du droit de rétractation sont, dans ce cas, à la charge du fournisseur et le consommateur doit en être informé. Dans de tels cas, la fourniture d'un bien ou d'un service ne peut être assimilée à une fourniture non demandée au sens de l'article 9.

Article 8 : paiement par carte

Les États membres veillent à ce que des mesures appropriées existent pour que le consommateur :
- puisse demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte de paiement dans le cadre de contrats à distance couverts par la présente directive ;
- en cas d'utilisation frauduleuse, soit recrédité des sommes versées en paiement ou se les voie restituées.

Article 9 : fourniture non demandée

Les États membres prennent les mesures nécessaires pour :
- interdire la fourniture de biens ou de services à un consommateur sans commande préalable de celui-ci, lorsque cette fourniture comporte une demande de paiement ;
- dispenser le consommateur de toute contre-prestation en cas de fourniture non demandée, l'absence de réponse ne valant pas consentement.

Article 10 : limites à l'utilisation de certaines techniques de communication à distance.

1] L'utilisation par un fournisseur des techniques suivantes nécessite le consentement préalable du consommateur :
- système automatisé d'appel sans intervention humaine (automate d'appel) ;
- télécopieur.

2) Les États membres veillent à ce que les techniques de communication à distance, autres que celles visées au paragraphe 1, lorsqu'elles permettent une communication individuelle, ne puissent être utilisées qu'en l'absence d'opposition manifeste du consommateur.

Article 11 : recours judiciaire ou administratif

1) Les États membres veillent à ce qu'il existe des moyens adéquats et efficaces pour faire respecter les dispositions de la présente directive dans l'intérêt des consommateurs.

2) Les moyens visés au paragraphe 1 comprennent des dispositions permettant à l'un ou plusieurs des organismes suivants, tels que déterminés par la législation nationale, de saisir selon le droit national les tribunaux ou les organismes administratifs compétents pour faire appliquer les dispositions nationales destinées à la mise en œuvre de la présente directive.

a) les organismes publics ou leurs représentants ;

b) les organisations de consommateurs ayant un intérêt légitime à protéger les consommateurs ;

c) les organisations professionnelles ayant un intérêt légitime à agir.

3) a) Les États membres peuvent établir que la production de la preuve de l'existence d'une information préalable, d'une confirmation écrite ou du respect des délais et du consentement du consommateur peut être à la charge du fournisseur.

b) Les États membres prennent les mesures nécessaires pour que les fournisseurs, ainsi que les opérateurs de techniques de communication lorsqu'ils sont en mesure de le faire, mettent fin aux pratiques non conformes aux dispositions prises en application de la présente directive.

4) Les États membres peuvent prévoir que le contrôle volontaire du respect des dispositions de la présente directive confié à des organismes autonomes et le recours à de tels organismes pour la solution de litiges s'ajoutent aux moyens que les États membres doivent prévoir pour assurer le respect des dispositions de la présente directive.

Article 12 : caractère contraignant des dispositions

1) Le consommateur ne peut renoncer aux droits qui lui sont conférés en vertu de la transposition en droit national de la présente directive.

2) Les États membres prennent les mesures nécessaires pour que le consommateur ne soit pas privé de la protection accordée par la présente directive du fait du choix du

droit d'un pays tiers comme droit applicable au contrat, lorsque le contrat présente un lien étroit avec le territoire d'un ou de plusieurs des États membres.

Article 13 : règles communautaires

1) Les dispositions de la présente directive s'appliquent pour autant qu'il n'existe pas, dans le cadre de réglementations communautaires, des dispositions particulières qui régissent certains types de contrats à distance dans leur globalité.

2) Lorsqu'une réglementation communautaire spécifique contient des dispositions qui ne régissent que certains aspects de la fourniture de biens ou de services, ces dispositions s'appliquent, de préférence aux dispositions de la présente directive, à ces aspects précis des contrats à distance.

Article 14 : clause minimale

Les États membres peuvent adopter ou maintenir, dans le domaine régi par la présente directive, des dispositions plus strictes compatibles avec le traité, pour assurer un niveau de protection plus élevé au consommateur. Ces dispositions comprennent, le cas échéant, l'interdiction, pour des raisons d'intérêt général, de la commercialisation sur leur territoire par voie de contrats à distance de certains biens ou services, notamment des médicaments, dans le respect du traité.

Article 15 : mise en œuvre

1) Les États membres mettent en vigueur les dispositions législatives, réglemen taires et administratives nécessaires pour se conformer à la présente directive au plus tard trois ans après son entrée en vigueur. Ils en informent immédiatement la Commission.

2) Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

3) Les États membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

4) Au plus tard quatre ans après l'entrée en vigueur de la présente directive, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente directive, accompagné, le cas échéant, d'une proposition de révision de la présente directive.

Article 16 : information du consommateur

Les États membres prennent les mesures appropriées pour informer le consommateur sur la législation nationale transposant la présente directive et incite, le cas échéant, les organisations professionnelles à informer les consommateurs sur leurs codes de pratique.

Article 17 : systèmes de réclamations

La Commission étudie la possibilité de mettre en place des moyens efficaces pour traiter les réclamations des consommateurs en matière de ventes à distance. Dans les deux ans suivant l'entrée en vigueur de la présente directive, la Commission soumet un rapport au Parlement européen et au Conseil sur les résultats des études réalisées, en l'accompagnant, le cas échéant, des propositions appropriées.

Article 18

La présente directive entre en vigueur le jour de sa publication au Journal officiel des Communautés européennes.

Article 19

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 20 mai 1997. Par le

Parlement européen

Le président J.M. Gil-Robles

Par le Conseil

Le président J. Van Aartsen

Annexe 1

Techniques de communication visées à l'article 2 point 4 :

— imprimé non adressé ;
— imprimé adressé ;
— lettre standardisée ;
— publicité presse avec bon de commande ;
— catalogue ;
— téléphone avec intervention humaine ;
— téléphone sans intervention humaine (automate d'appel, audiotexte) ;
— radio ;
— visiophone (téléphone avec image) ;
— vidéotexte (micro-ordinateur, écran de télévision) avec clavier ou écran tactile ;
— courrier électronique ;
— télécopieur ;
— télévision (téléachat, télévente).

Annexe 2

Services financiers visés à l'article 3 paragraphe 1 :

— services d'investissement ;
— opérations d'assurance et de réassurance ;
— services bancaires ;
— opérations ayant trait aux fonds de pensions ;
— services visant des opérations à terme ou en option.

Ces services comprennent en particulier :

— les services d'investissement visés à l'annexe de la directive 93/22/CEE [1] , les services d'entreprises d'investissements collectifs ;

[1] JO n° L 141 du 11 juin 1993, p. 27.

- les services relevant des activités bénéficiant de la reconnaissance mutuelle et visés à l'annexe de la directive 89/646/CEE [1] ;
- les opérations relevant des activités d'assurance et de réassurance visées : à l'article 1er de la directive 73/239/CEE [2] ;
- à l'annexe de la directive 79/267/ŒE [3] ;
- par la directive 64/225/CEE [4] ;
- par les directives 92/49/CEE [5] et 92/96/CEE [6].

Déclaration du Conseil et du Parlement européen sur l'article 6 paragraphe 1

Le Conseil et le Parlement européen notent que la Commission examinera la possibilité et l'opportunité d'harmoniser la méthode de calcul du délai de réflexion dans le cadre de la législation existante en matière de protection des consommateurs, notamment la directive 85/577/ŒE, du 20 décembre 1985, concernant la protection des consommateurs dans le cas de contrats négociés en dehors des établissements commerciaux (démarchage à domicile) [7]

Déclaration de la Commission sur l'article 3 paragraphe I premier tiret

La Commission reconnaît l'importance que revêt la protection des consommateurs en matière de contrats à distance portant sur les services financiers et elle a d'ailleurs publié un livre vert intitulé « Services financiers : répondre aux attentes des consommateurs ». À la lumière des réactions que suscitera le livre vert, la Commission examinera les moyens d'intégrer la protection des consommateurs dans la politique ayant trait aux services financiers et les éventuelles incidences législatives et, au besoin, présentera des propositions appropriées.

1 *JO* n° L 386 du 30 décembre 1989, p. 1. Directive modifiée par la direc ive 92/30/CEE (*JO* n° L 110 du 28 avril 1992, p. 52).
2 *JO* n° L 228 du 16 août 1973, p. 3. Direc ive modifiée en dernier lieu par la direc ive 92/49/CEE (*JO n"* L 228 du 11 août 1992, p. 1).
3 JO n° L 63 du 13 mars 1979, p. 1. Directive modifiée en dernier lieu par la direc ive 90/619/CEE (JO n° L 330 du 29 novembre 1990, p. 50).
4 *JO* n° 56 du 4 avril 1964, p. 878/64. Directive modifiée par l'acte d'adhésion de 1973.
5 JO n° L 228 du 11 août 1992, p. 1.
6 JO n° L 360 du 9 décembre 1992, p. 1.
7 *JO* n° L 372 du 31 décembre 1985, p. 31.

Annexe 9

Recommandation n° R (97) 5, du Comité des ministres aux États membres relative à la protection des données médicales

adoptée par le Comité des ministres le 13 février 1997, lors de la 584e réunion des délégués des ministres

Le Comité des ministres, en vertu de l'article 15. b du statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Rappelant les principes généraux relatifs à la protection des données de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (série des traités européens, no 108), notamment son article 6 qui énonce que les données à caractère personnel relatives à la santé ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées ;

Conscient du fait que le traitement automatisé des données médicales par des systèmes d'information est de plus en plus répandu non seulement pour les soins médicaux, la recherche médicale, la gestion hospitalière et la santé publique, mais également en dehors du secteur des soins de santé ;

Convaincu de l'importance que la qualité, l'intégrité et la disponibilité des données médicales revêtent pour la santé de la personne concernée et de ses proches ;

Conscient du fait que les progrès des sciences médicales dépendent dans une large mesure de la disponibilité des données médicales des individus ;

Persuadé qu'il est souhaitable de réglementer la collecte et le traitement des données médicales, de garantir le caractère confidentiel et la sécurité des données à caractère personnel relatives à la santé, et de veiller à ce qu'il en soit fait un usage respectant les droits et les libertés fondamentales de l'individu, notamment le droit à la vie privée ;

Conscient du fait que les progrès accomplis dans les sciences médicales et les développements intervenus dans la technologie de l'information depuis 1981 nécessitent la révision de plusieurs dispositions de la recommandation no R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées,

Recommande aux gouvernements des États membres :

— de prendre des mesures pour que les principes contenus dans l'annexe à la présente recommandation se reflètent dans leur droit et leur pratique ;

— d'assurer une large diffusion des principes contenus dans l'annexe à la présente recommandation parmi les personnes qui collectent et traitent des données médicales à titre professionnel.

Décide que la présente recommandation remplace la recommandation no R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées.

Annexe à la recommandation n° R (97) 5

1) Définitions

Aux fins de la présente recommandation :

— l'expression « données à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais et des activités

déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes ;

— l'expression « données médicales » se réfère à foutes les données à caractère personnel relatives à la santé d'une personne. Elle se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques ;

— l'expression « données génétiques » se réfère à toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés.

Elle se réfère également à toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable.

La lignée génétique est constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus.

2) Champ d'application

2.1) La présente recommandation est applicable à la collecte et au traitement automatisé de données médicales, à moins que le droit interne, dans un contexte spécifique hors du domaine des soins de santé, ne prévoie d'autres garanties appropriées.

2.2) Un État membre peut étendre les principes énoncés dans la présente recommandation aux données médicales ne faisant pas l'objet d'un traitement automatisé.

3) Respect de la vie privée

3.1) Le respect des droits et des libertés fondamentales, notamment du droit à la vie privée, doit être garanti lors de la collecte et du traitement des données médicales.

3.2) Les données médicales ne peuvent être collectées et traitées que conformément aux garanties appropriées qui doivent être prévues par le droit interne.

En principe, la collecte et le traitement de données médicales ne devraient être effectués que par des professionnels des soins de santé ou par des personnes ou organismes agissant pour le compte de professionnels des soins de santé. Les personnes ou organismes agissant pour le compte de professionnels des soins de santé qui collectent et traitent des données médicales devraient être soumis aux règles de confidentialité propres aux professionnels des soins de santé ou à des règles de confidentialité comparables.

Les maîtres des fichiers qui ne sont pas des professionnels des soins de santé ne devraient collecter et traiter des données médicales que dans le respect soit de règles de confidentialité comparables à celles incombant à un professionnel des soins de santé, soit des garanties d'efficacité égales prévues par le droit interne.

4) Collecte et traitement de données médicales

4.1) La collecte et le traitement des données médicales doivent être effectués de manière loyale et licite, et uniquement pour des finalités déterminées.

4.2) Les données médicales doivent en principe être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 4, 6 et 7 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données.

4.3) Les données médicales peuvent être collectées et traitées :

a) si la loi le prévoit :
- aux fins de la santé publique ; ou
- sous réserve du principe 4.8, aux fins de la prévention d'un danger concret ou pour la répression d'une infraction pénale déterminée ; ou
- aux fins d'un autre intérêt public important ; ou

b) dans la mesure où la loi l'autorise :
- à des fins médicales préventives, ou à des fins diagnostiques ou thérapeutiques à l'égard de la personne concernée ou d'un parent de la lignée génétique ; ou
- aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une tierce personne ; ou
- aux fins du respect d'une obligation contractuelle spécifique ; ou
- aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice ; ou

c) si la personne concernée ou son représentant légal, ou une autorité, ou toute personne ou instance désignée par la loi y a consenti, pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas.

4.4) Lorsque les données médicales ont été collectées à des fins médicales préventives, ou à des fins diagnostiques ou thérapeutiques à l'égard de la personne concernée ou d'un parent de la lignée génétique, elles peuvent également être traitées à des fins de gestion d'un service de santé agissant dans l'intérêt au patient, dans le cas où la gestion est fournie par le professionnel des soins de santé qui a collecté les données, ou lorsque les données sont communiquées conformément aux dispositions énoncées aux principes 7.2 et 7.3.

Enfant à naître

4.5) Les données médicales relatives à un enfant à naître devraient être considérées comme des données à caractère personnel et jouir d'une protection compa rable à celle des données médicales d'un mineur.

4.6) À moins que le droit interne n'en dispose autrement, le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir pour un enfant à naître en tant que personne concernée.

Données génétiques

4.7) Les données génétiques collectées et traitées à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou pour la recherche scientifique ne devraient être utilisées qu'à ces seules fins ou pour permettre à la personne concernée de prendre une décision libre et éclairée à leur sujet.

4.8) Le traitement des données génétiques pour les besoins d'une procédure judiciaire ou d'une enquête pénale devrait faire l'objet d'une loi spécifique offrant des garanties appropriées.

Ces données devraient servir exclusivement à la vérification de l'existence d'un lien génétique dans le cadre de l'administration de la preuve, à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. En aucun cas elles ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

4.9) A des fins autres que celles prévues aux principes 4.7 et 4.8, la collecte et le traitement des données génétiques devraient en principe être permis uniquement pour des raisons de santé et notamment pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers.

Cependant, la collecte et le traitement des données génétiques en vue de dépister des maladies peuvent être permis en cas d'intérêt supérieur et à condition qu'il existe des garanties appropriées définies par la loi.

5) Information de la personne concernée

5.1) La personne concernée doit être informée des éléments suivants :
a) l'existence d'un fichier contenant ses données médicales et la catégorie de données collectées ou à collecter ;
b) la ou les finalités pour lesquelles ces données sont ou seront traitées ;
c) le cas échéant, les personnes ou les organismes auprès desquels elles sont ou seront collectées ;
d) les personnes ou les organismes auxquels — et les objectifs pour lesquels — elles peuvent être communiquées ;
e) la possibilité, le cas échéant, pour la personne concernée de refuser son consentement, de le retirer, et les conséquences d'un tel retrait ;
f) l'identité du maître de fichier et, le cas échéant, de son représentant, ainsi que les conditions d'exercice du droit d'accès et de rectification.

5.2) La personne concernée devrait être informée au plus tard au moment de la collecte. Toutefois, lorsque les données médicales ne sont pas collectées auprès de la personne concernée, celle-ci devrait être informée de la collecte le plus rapidement possible ainsi que, de manière appropriée, des éléments mentionnés au principe 5.1, sauf si cela est manifestement déraisonnable ou infaisable, ou si la personne concernée a déjà reçu l'information.

5.3) L'information de la personne concernée doit être appropriée et adaptée aux circonstances. Chaque personne concernée devrait, de préférence, être informée indivi duellement.

5.4) Avant qu'une analyse génétique soit effectuée, la personne concernée devrait être informée des objectifs de l'analyse et de l'éventualité de découvertes inattendues.

Incapables légaux

5.5) Si la personne concernée est une personne légalement incapable et n'est pas en mesure de se déterminer librement, et si le droit interne ne lui permet pas d'agir en son propre nom, l'information doit être donnée à la personne pouvant agir légalement dans l'intérêt de la personne concernée.

Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient collectées ou traitées.

Dérogations

5.6) Des dérogations aux principes 5.1, 5.2 et 5.3 peuvent être faites dans les cas suivants :
a) l'information de la personne concernée peut être limitée, si la dérogation est prévue par la loi et qu'elle constitue une mesure nécessaire dans une société démocratique :
— à la prévention d'un danger concret ou à la répression d'une infraction pénale ;
— pour des raisons de santé publique ;
— à la protection de la personne concernée et des droits et libertés d'autrui ;
b) en cas d'urgence médicale, les données considérées comme étant nécessaires au traitement médical peuvent être collectées avant l'information.

6) Consentement

6.1) Lorsque la personne concernée est appelée à donner son consentement, celui-ci devrait être libre, exprès et éclairé.

6.2) Les résultats de toute analyse génétique devraient être formulés dans les limites des objectifs de la consultation médicale, au diagnostic ou du traitement pour lesquels le consentement a été obtenu.

6.3) Lorsque l'on envisage de traiter des données médicales concernant une personne légalement incapable qui n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne permet pas à la personne concernée d'agir en son propre nom, le consentement de la personne pouvant agir légalement au nom de la personne concernée, ou d'une autorité, ou de toute personne ou instance désignée par la loi, est requis.

Si, conformément au principe *5.5* ci-dessus, la personne légalement incapable a été informée de l'intention de collecter ou de traiter ses données médicales, son souhait devrait être pris en considération, à moins que le droit interne ne s'y oppose.

7) Communication

7.1) Les données médicales ne doivent pas être communiquées, sauf dans les conditions énumérées dans le cadre du présent principe et du principe 12.

7.2) En particulier, à moins que le droit interne ne prévoie d'autres garanties appropriées, la communication des données médicales ne peut intervenir que si le destinataire est soumis aux règles de confidentialité propres aux professionnels des soins de santé ou à des règles de confidentialité comparables, et seulement s'il respecte les dispositions de la présente recommandation.

7.3) Les données médicales peuvent être communiquées si elles sont pertinentes et:

a) si la communication est prévue par la loi et constitue une mesure nécessaire dans une société démocratique aux fins :
— de la santé publique ; ou
— de la prévention d'un danger concret ou pour la répression d'une infraction pénale déterminée ; ou
— d'un autre intérêt public important ; ou
— de la protection des droits et libertés d'autrui ; ou

b) si la loi autorise la communication aux fins :
— de la protection de la personne concernée ou d'un parent de la lignée génétique ; ou
— de la sauvegarde des intérêts vitaux de la personne concernée ou d'une tierce personne ; ou
— du respect d'obligations contractuelles spécifiques ; ou
— de la constatation, de l'exercice ou de la défense d'un droit en justice ; ou

c) si la personne concernée ou son représentant légal, ou une autorité, ou toute personne ou instance désignée par la loi y a consenti pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas ;

d) à moins que la personne concernée ou son représentant légal, ou une autorité, ou toute personne ou instance désignée par la loi ne s'y soit expressément opposée lorsque la communication n'est pas obligatoire, si les données ont été collectées dans un contexte préventif, diagnostique ou thérapeutique librement choisi, et si la finalité de la communication n'est pas incompatible avec la finalité du traitement pour laquelle ces données ont été collectées, notamment aux fins d'accomplissement de soins au patient ou de gestion d'un service de santé agissant dans l'intérêt du patient.

8) Droits de la personne concernée

Droits d'accès et de rectification

8.1) Toute personne doit pouvoir accéder aux données médicales la concernant, soit directement, soit par l'intermédiaire d'un professionnel des soins de santé, ou, si le droit interne le permet, par l'intermédiaire d'une personne désignée par elle. Les informations doivent être accessibles sous une forme compréhensible.

8.2) L'accès aux données médicales peut être refusé, limité ou différé uniquement si la loi le prévoit, et :

a) si cela constitue une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique ou à la répression des infractions pénales ; ou

b) si la connaissance de *ces* informations est susceptible de causer une atteinte grave à la santé de la personne concernée ; ou

c) si l'information sur la personne concernée révèle également des informations sur des tiers, ou, en ce qui concerne les données génétiques, si ces informations sont susceptibles de porter une atteinte grave à des parents consanguins ou utérins, ou à une personne ayant un lien direct avec cette lignée génétique ; ou

d) si les données sont utilisées à des fins de statistiques ou de recherches scientifiques lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées, notamment du fait que les données ne sont pas utilisées pour des décisions ou des mesures relatives à une personne déterminée.

8.3) La personne concernée peut demander la rectification de données erronées la concernant et, en cas de refus, doit pouvoir faire recours.

Découvertes inattendues

8.4) La personne soumise à une analyse génétique devrait être informée des découvertes inattendues si les conditions suivantes ont été remplies :

a) le droit interne n'interdit pas une telle information ;

b) la personne a fait la demande explicite de cette information ;

c) l'information n'est pas susceptible de porter une atteinte grave :

— à la santé de la personne ; ou

— à un parent consanguin ou utérin de la personne, à un membre de sa famille sociale, ou à une personne ayant un lien direct avec la lignée génétique de la personne, à moins que le droit interne ne prévoie d'autres garanties appropriées.

Sous réserve de l'alinéa a), la personne devrait également être informée si ces découvertes revêtent pour elle une importance thérapeutique ou préventive directe.

9) Sécurité

9.1) Des mesures techniques et d'organisation appropriées doivent être prises pour la protection des données à caractère personnel traitées conformément à la présente recommandation contre la destruction — accidentelle ou illicite — et la perte accidentelle, ainsi que contre l'accès, la modification, la communication ou toute autre forme de traitement non autorisés.

Ces mesures doivent assurer un niveau de sécurité approprié compte tenu, d'une part, de l'état de la technique et, d'autre part, de la nature sensible des données médicales et de l'évaluation des risques potentiels.

Ces mesures doivent faire l'objet d'un examen périodique.

9.2) Afin notamment d'assurer la confidentialité, l'intégrité et l'exactitude des données traitées, ainsi que la protection des patients, des mesures appropriées devraient être prises visant :

a) à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations) ;

b) à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données) ;

e) à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire) ;

d) à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation) ;

e) en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation :

— des identifiants et des données relatives à l'identité des personnes ;
— des données administratives ;
— des données médicales ;
— des données sociales ;
— des données génétiques (contrôle d'accès) ;

f) à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication) ;

g) à garantir qu'il puisse être vérifié et constaté a *posteriori* qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction) ;

h) à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport) ;

i) à sauvegarder les données par la constitution de copies de sécurité (contrôle de disponibilité).

9.3) Les maîtres des fichiers médicaux devraient, conformément au droit interne, établir un règlement interne approprié dans le respect des principes pertinents de la présente recommandation.

9.4) Si nécessaire, les maîtres des fichiers qui traitent des données médicales devraient désigner une personne indépendante responsable de la sécurité des systèmes d'information et de la protection des données, et compétente pour donner des conseils en la matière.

10) Conservation

10.1) En règle générale, les données médicales ne doivent être conservées que pendant la durée nécessaire pour atteindre le but pour lequel elles ont été collectées et traitées.

10.2) Lorsque la conservation de données médicales qui ne sont plus utilisées pour le but d'origine se révèle nécessaire dans l'intérêt légitime de la santé publique, de la science médicale, du responsable du traitement médical ou du maître du fichier aux fins de lui permettre d'exercer ou de défendre ses droits en justice, ou à des fins historiques ou statistiques, des dispositions techniques doivent être prises pour assurer la conservation et la sécurité correctes des données en tenant compte de la vie privée du patient.

10.3) Sur demande de la personne concernée, ses données médicales devraient être effacées, à moins qu'elles ne soient rendues anonymes ou que des intérêts supérieurs et légitimes, et en particulier ceux énoncés au principe 10.2, ou des obligations d'archivage ne s'y opposent.

11) Flux transfrontières

11.1) Les principes de la présente recommandation sont applicables aux flux transfrontières de données médicales.

11.2) Les flux transfrontières de données médicales vers un État ayant ratifié la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et disposant d'une législation qui assure une protection des données médicales pour le moins équivalente, ne devraient pas être soumis à des conditions particulières de protection de la vie privée.

11.3) Lorsque la protection des données médicales peut être considérée comme étant en harmonie avec le principe de la protection équivalente énoncé dans ladite convention, il ne devrait pas y avoir de limitation aux flux transfrontières de données médicales vers un État n'ayant pas ratifié la convention, mais assurant une protection conforme aux principes de ladite convention et de la présente recommandation.

11.4) À moins que le droit interne n'en dispose autrement, les flux transfrontières de données médicales vers un État n'assurant pas une protection conforme à ladite convention et à la présente recommandation ne devraient en règle générale pas intervenir, à moins :

a) que des mesures nécessaires, y compris de nature contractuelle, au respect des principes de la convention et de la présente recommandation n'aient été prises et que la personne concernée n'ait la possibilité de s'opposer au transfert ; ou

b) que la personne concernée n'ait donné son consentement.

11.5) Sauf en cas d'urgence ou de transfert accepté par la personne concernée après information, lorsque des données médicales sont transférées d'un pays à un autre, des mesures appropriées devraient être prises pour assurer leur protection, en particulier :

a) le responsable au transfert devrait indiquer au destinataire les finalités déterminées et légitimes pour lesquelles les données ont été initialement collectées, ainsi que les personnes ou organismes auxquels elles peuvent être communiquées ;

b) sauf si le droit interne en dispose autrement, le destinataire devrait s'engager auprès du responsable du transfert à respecter les finalités déterminées et légitimes reconnues, et à ne pas communiquer ces données à des personnes ou organismes autres que ceux indiqués par le responsable du transfert.

12) Recherche scientifique

12.1) Dans la mesure du possible, les données médicales utilisées à des fins de recherche scientifique devraient être anonymes. Les organisations professionnelles et scientifiques ainsi que les autorités publiques devraient promouvoir le développement de techniques et de procédures assurant l'anonymat.

12.2) Toutefois, si l'anonymisation devait rendre impossible un projet de re cherche scientifique et si ce projet devait être effectué dans un but légitime, la recherche pourrait être faite avec des données à caractère personnel, à condition :

a) que la personne concernée ait donné son consentement informé pour la ou les finalités de la recherche ; ou

b) que, lorsque la personne concernée est légalement incapable et n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne lui permet pas d'agir en son

propre nom, son représentant légal ou une autorité, ou toute personne ou instance désignée par la loi, ait donné son consentement dans le cadre d'un projet de recherche lié à la condition médicale ou à une maladie de la personne concernée ; ou

c) que la communication des données aux fins d'un projet de recherche scientifique déterminé pour des raisons d'intérêt public importantes ait été autorisée par un ou plusieurs organismes désignés par le droit interne, mais seulement :

- si la personne concernée ne s'est pas expressément opposée à la communication ; et
- s'il s'avère irréalisable, malgré des efforts raisonnables, de prendre contact avec la personne concernée pour recueillir son consentement ; et
- si les intérêts du projet de recherche justifient cette autorisation ; ou

d) que la recherche scientifique soit prévue par la loi et qu'elle constitue une mesure nécessaire pour des raisons de santé publique.

12.3) Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels des soins de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données médicales qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée.

12.4) À l'égard de toute recherche scientifique fondée sur des données à caractère personnel, les problèmes incidents engendrés par le respect des dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, y compris ceux de nature éthique et scientifique, devraient également être examinés à la lumière d'autres instruments pertinents.

12.5) Les données à caractère personnel utilisées à des fins de recherche scientifique ne peuvent être publiées sous une forme permettant d'identifier les personnes concernées à moins que ces dernières n'aient donné leur consentement en vue de la publication et que le droit interne autorise cette publication.

Annexe 10

Actualité parlementaire

ÉCONOMIE

Incidents de paiement

45645 — 25 novembre 1996 — **Monsieur Jean-Michel Dubernard** attire l'attention de **Monsieur le ministre de l'Économie et des Finances** sur la situation suivante : Chaque citoyen titulaire d'un compte postal ou bancaire est inscrit à la Banque de France, sous deux critères : Celui de l'utilisation des chèques et celui du comportement quant aux remboursements des crédits souscrits. Il existe trois notations pour chacun des critères : 000 (rien à signaler) ; 050 (incidents de paiement ou règlement, non autorisé par l'établissement bancaire du titulaire) : 060 (incidents répétés). En cas de chèque émis, non provisionné et sans accord de découvert, la banque gérant le compte informe la Banque de France d'un incident de paiement. Cet incident de paiement fait alors l'objet d'une notation. L'information est mise à la disposition des banques, qui peuvent ainsi juger les clients demandeurs d'ouverture de comptes. La notation 050 entraîne une surveillance accrue du titulaire, éventuellement le refus de tous concours bancaires, de toutes facilités de caisse et disparaît sur demande de la Banque de Gestion du compte signalé après effacement de l'incident par le titulaire du compte et accord de la banque. La notation restera de toute façon inscrite, même si elle est levée, permettant ainsi aux établissements bancaires de disposer d'un historique. La notation 060 entraîne le blocage du compte du titulaire, le retrait du chéquier, le refus de tous concours bancaires. En aucun cas le demandeur d'ouverture de compte n'est prévenu de cette surveillance, ni de cette notation, encore moins des conséquences encourues.

Enfin, lorsqu'une société dépose son bilan et est mise en liquidation, sur simple information à partir des publicités inscrites dans les journaux légaux, la Banque de France note à 050 le responsable de la société, au titre de la société. La société n'existe plus, puisqu'elle est mise en liquidation par le tribunal de commerce, mais l'inscription reste pendant cinq ans... Une demande de réduction d'inscription peut être engagée auprès du gouverneur de la Banque de France, lequel accordera peut être, une réduction d'inscription d'un mois au maximum !... De ce fait, on interdit pratiquement pendant cinq ans au particulier, ancien responsable de société, de solliciter un concours bancaire, bien que certaines banques ne tiennent compte que des cotisations personnelles du demandeur, et en tout cas à un entrepreneur honnête de pouvoir recréer, en tant que responsable, une quelconque entreprise demandant un concours bancaire. La Commission nationale de l'informatique et des libertés considère ce comportement comme anormal mais n'a pas d'autorité pour agir auprès de la Banque de France. Il lui demande quelles mesures il pense prendre pour pallier cet état de fait.

Réponse. — La Banque de France a reçu du législateur la mission de gérer plusieurs fichiers dont les vocations sont différentes. Certains fichiers concernent les incidents de paiement, tandis que d'autres centralisent des données sur les moyens de paiement, et tout particulièrement les chèques sans provision. Par ailleurs, il convient de distinguer les fichiers rassemblant des informations relatives aux particuliers des bases de données concernant les entreprises. Institué par la loi n° 89-1010 du 31 décembre 1989 relative à la prévention et au règlement des difficultés liées au surendettement des particuliers et des familles, le fichier national des incidents de remboursement des crédits aux particuliers (FICP) est régi par le règlement n° 90-05 du 11 avril 1990 du comité de la réglementation bancaire, modifié par le règlement n° 96-04 du 24 Mai 1996. Ce fichier, géré de façon centralisée par la Banque de France, est destiné au recensement

des informations sur les incidents de paiement caractérisés survenus à l'occasion du remboursement des crédits accordés à des personnes physiques. Ses informations sont réservées à l'usage exclusif des établissements de crédit, qui ne peuvent les utiliser que dans le cadre d'opérations se rattachant à l'octroi ou à la gestion d'un crédit. Bien entendu, le dispositif prévoit l'information des emprunteurs tant en ce qui concerne leur inscription au fichier que leur radiation. En premier lieu, l'article 4 du règlement n° 90-05 du 11 Avril 1990 impose à l'établissement de crédit, dès qu'un incident de paiement caractérisé est constaté, d'informer le débiteur défaillant que l'incident sera déclaré à la Banque de France à l'issue d'un délai d'un mois à compter de la date de l'envoi de cette information. Au terme de ce délai, sauf si les sommes dues ont été réglées ou si une solution amiable a été trouvée, le débiteur défaillant est informé par l'établissement de crédit de la teneur des informations (limitativement énumérées par l'article 5 dudit règlement) que ce dernier transmet à la Banque de France. En ce qui concerne la radiation du fichier, l'article 8 alinéa 3 du règlement n° 90-05 du 11 avril 1990 dispose que les informations sont radiées dès la date d'enregistrement dans le fichier de la déclaration du paiement intégral des sommes dues.

Cette déclaration est faite par les établissements de crédit à la Banque de France, pour chaque incident de paiement précédemment déclaré, en application de l'article 6 du même règlement.

Pour les personnes qui souhaiteraient savoir si elles sont inscrites ou non au FICP, l'article 13 du règlement précité prévoit expressément l'exercice du droit d'accès tel qu'affirmé par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le guichet de la Banque de France, saisi de cette demande, communique alors oralement à la personne intéressée les informations qui la concernent. Le titulaire du droit d'accès peut, le cas échéant, obtenir la modification des informations le concernant. Pour ce qui est des entreprises industrielles et commerciales, les informations relatives aux incidents de paiement sont rassemblées au sein d'une base de données nationale intitulée fichier bancaire des entreprises (FIBEN). Une cotation est en effet attribuée aux entreprises, qui fait l'objet d'un enregistrement dans la base de données, et constitue un critère de classement des créances privées éligibles aux interventions de l'institut d'émission. La Banque de France accepte en effet de refinancer les crédits à moins de deux ans accordés aux entreprises bénéficiant de sa cotation la plus favorable. Cette cotation résume l'appréciation globale portée sur l'entreprise concernée par les services de la Banque de France à l'aide de trois éléments : Une cote d'activité, une cote de crédit et une cote de paiement. Toutefois, il est important de souligner que cette occasion, communiquée aux établissements de crédit qui interrogent la Banque de France mais non accessible au public, ne lie en aucun cas l'établissement de crédit, qui demeure libre de consentir ou non des concours à une entreprise, quelle que soit la cote attribuée par la Banque de France. Le prêteur dispose en effet de sa propre grille d'analyse et peut faire usage de multiples sources de renseignements avant de prendre sa décision d'octroi ou de refus. En outre, il convient d'ajouter que les représentants légaux d'une entreprise bénéficient d'un droit d'accès et de rectification des informations détenues à leur nom par la Banque de France dans la base de données FIBEN, conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Enfin, la Banque de France a reçu du législateur, en vertu de l'article 4 de ses statuts, la mission de veiller au bon fonctionnement et à la sécurité des systèmes de paiement. A ce titre, la loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement a sensiblement renforcé le rôle des fichiers gérés par la Banque de France dans le dispositif préventif de lutte contre l'émission de chèques sans provision et de chèques irréguliers. Ainsi, dans le dispositif actuel, l'émetteur de chèque sans provision est immédiatement déclaré à la Banque de France dès le premier incident. Il est aussitôt

interdit bancaire et peut rester recensé dans le fichier central des chèques (FCC) dix ans. Toutefois, l'interdit bancaire peut, à tout moment, recouvrer la capacité d'émettre des chèques et obtenir sa radiation du fichier par la régularisation des chèques sans provision émis, assorties, le cas échéant, du paiement d'une pénalité libératoire, dont le montant est fixé par la loi à 120 francs par tranche de 1 000 francs ou fraction de tranche. Par ailleurs, la loi du 30 décembre 1991 précitée a institué un fichier national des chèques irréguliers (FNCI), qui recense les chèques perdus, volés, falsifiés, tirés sur un compte clôturé ou émis par un interdit bancaire.

Assemblée nationale 17 mars 1997 n° 11 (p. 1365)

ETRANGERS

Demandes de visa

1711 — 24 juillet 1997 — **M. Bernard Plasait** attire l'attention de **Monsieur le ministre de l'Intérieur** sur l'intérêt de créer un fichier dactyloscopique des demandes de visa qui permettrait d'identifier tous les étrangers entrés en France munis d'un visa et qui seraient maintenus sur le territoire à l'expiration de leur titre de séjour. Les empreintes des demandeurs de visa pourraient être prises dans les pays qui présentent un risque migratoire. Les consulats pourraient dispenser de cette formalité les ressortissants de pays la prévoyant pour la délivrance de documents d'identité — donc de pays eri mesure d'identifier leurs ressortissants, ainsi que des personnes présentant certaines garanties (universitaires, responsables politiques, hommes d'affaires, etc.). Il lui demande donc de bien vouloir lui préciser ses intentions sur ce sujet.

Réponse. — L'honorable parlementaire propose la constitution d'un fichier des empreintes digitales des demandeurs de visa. Sans négliger son utilité pour l'identification des étrangers en situation irrégulière, ce fichier impliquerait un équipement de tous nos consulats et représenterait un système lourd et coûteux. En outre, la France serait le seul pays à procéder à un tel relevé dactyloscopique. La proposition de création d'un fichier dactyloscopique des demandes de visa limité, d'une part, aux pays qui présentent un risque migratoire et n'ont pas de dispositif de relevé d'empreintes pour la délivrance de leurs documents d'identité et, d'autre part, aux étrangers ne disposant pas de certaines garanties (universitaires, responsables politiques, hommes d'affaires, etc.) présente d'autres difficultés qui rendent ce fichier également difficilement envisageable. Un fichier sélectif risquerait d'être ressenti comme une suspicion à l'encontre des Etats qui y seraient soumis et cela pourrait contribuer à la dégradation de nos relations avec le pays en question. L'existence de ce fichier pourrait, en outre, induire des détournements de demande de visa de court séjour vers les consulats des autres États parties à la Convention de Schengen. En effet, pour être réellement efficace, la création d'un tel fichier dacfyloscopique devrait intervenir dans le cadre de la politique commune des visas définie par la Convention d'application de l'accord de Schengen. Des difficultés d'application apparaîtraient par ailleurs dans les postes consulaires compte tenu du nombre important de visas délivrés annuellement : Procédure de délivrance allongée, coût élevé. Les accords bilatéraux dont nous disposons actuellement dans le domaine de la circulation et du séjour des personnes devraient être renégociés, ces accords précisant limitativement les conditions applicables à la délivrance des visas. Il ne paraît, en conséquence, pas possible de réserver une suite favorable aux propositions de l'honorable parlementaire, d'une part, en raison des contraintes d'ordres financiers et techniques et, d'autre part, pour des raisons touchant aux relations diplomatiques de la France avec certains États.

Sénat 18 septembre 1997 n° 35 (p. 2476)

INTERNET

Annuaires professionnels

19832 — 2 janvier 1997 — **M. Emmanuel Hamel** attire l'attention de **Monsieur le ministre de l'Industrie, de la Poste et des Télécommunications su**r la proposition faite dans le seizième rapport annuel d'activité de la Commission nationale de l'informatique et des libertés (CNIL) rendu public le 8 juillet dernier et rapporté par le *Bulletin quotidien* du 9 juillet dernier, pages 21 et 22, de soumettre à deux conditions la mise en œuvre sur Internet d'annuaires professionnels de chercheurs : « que l'accord des chercheurs soit recueilli et que soient rappelés sur l'écran les droits, garantie et protections des individus, ainsi que l'interdiction de captage des informations à des fins d'enrichissement de bases de données commerciales et publicitaires ». Il lui demande quelle fut sa réaction face à cette proposition et s'il envisage de contribuer à la mettre en oeuvre.

Réponse. — L'architecture mondiale du réseau Internet constitue un instrument privilégié pour les communications et les échanges entre chercheurs du monde entier en favorisant le développement de la coopération internationale grâce à une connaissance amplifiée des personnes et des thèmes de recherche au sein de la Communauté scientifique internationale. La Commission nationale de l'informatique et des libertés (CNIL) s'est de ce fait trouvée saisie de plusieurs demandes d'avis relatives à la mise en œuvre d'annuaires professionnels de chercheurs. Or, la diffusion de ces annuaires par le biais de réseaux internationaux offrant une grande facilité d'accès, de consultation et de copie des informations suscite certaines difficultés au regard de la loi du 6 janvier 1978, et notamment de celles de ses dispositions relatives au principe de finalité, aux catégories de destinataires, à la sécurité et aux flux transfrontières. La CNIL a ainsi souhaité entourer de garanties suffisantes la mise en œuvre de ces traitements. A cette fin, elle a demandé que l'accord des chercheurs soit recueilli et qu'avant d'accéder aux informations nominatives recherchées, un avis rappelle aux utilisateurs des droits, garanties et protections des personnes figurant sur un annuaire ainsi que l'interdiction de captage des informations à des fins d'enrichissement de bases de données commerciales ou publicitaires. L'avis délivré par cette autorité, entourant des nécessaires garanties la mise en œuvre d'annuaires électroniques sur Internet, paraît avoir trouvé le juste point d'équilibre entre la liberté d'expression et la protection des personnes.

Sénat 1 3 mars 1997 n° 11 (p. 782)

LIBERTÉS PUBLIQUES

Refonte de la loi « Informatique et libertés »

46550 — 23 décembre 1996 — **M. Jean-Pierre Kucheida** appelle l'attention de **Monsieur le garde des Sceaux, ministre de la Justice,** sur la directive européenne du 24 octobre dernier obligeant les États membres à harmoniser, dans un délai de trois ans, les politiques nationales relatives à la circulation des données à caractère personnel. En effet, la France, pionnière en matière de protection des libertés face aux risques liés à l'informatisation, n'aurait en principe à apporter que quelques modifications à la législation en vigueur. Cependant, il semblerait que le projet envisagé par son ministère de la Justice de modifier le dispositif adopté en 1978 pour garantir les libertés face à la multiplication des fichiers aille bien au-delà des obligations communautaires et remettre en cause les prérogatives de la Commission nationale de l'informatique et des libertés, autorité indépendante chargée de la protection de la vie privée et des libertés. Or l'adaptation de la loi ne saurait souffrir d'une réduction des garanties assurées

par la loi de 1978, telle que l'accentuation du contrôle des administrations sur les citoyens, Il lui demande en conséquence de lui préciser ses intentions à ce sujet.

Réponse. — Le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que la directive n° 95/46/Œ 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 présente, par sa philosophie comme par les solutions qu'elle apporte, des différences profondes avec la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En effet, quand bien même certaines de ses dispositions ont pu être inspirées par les mécanismes de protection de la législation française, le texte communautaire s'efforce de répondre à la très grande diffusion dans la société que connaissent aujourd'hui les techniques informatiques et aux impératifs de circulation accrue des dossiers de données qui en résultent, en privilégiant le contrôle *a posteriori* des traitements automatisés. En contrepartie, la directive limite le champ des interventions a *priori* de l'autorité de contrôle aux seuls fichiers considérés comme susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes.

Elle n'opère à cet égard entre les traitements des secteurs public et privé aucune des distinctions effectuées par la loi informatique et libertés. Plus généralement, elle fait prévaloir l'énoncé de principes fondamentaux relatifs à la licéité des traitements sur les critères de forme tenant au respect des démarches procédurales exigibles des responsables de fichiers. Compte tenu des options ouvertes par la directive, le Gouvernement a demandé au Conseil d'État un rapport, dont les conclusions sont actuellement soumises à la concertation interministérielle. Sans préjuger des choix qui pourront être retenus par le Gouvernement, la loi de transposition devra instaurer un régime comportant, au regard des droits et libertés individuelles, un niveau de protection et de garanties équivalent à celui qui est présentement assuré par la loi informatique et libertés.

Assemblée nationale 3 février 1997 n° 5 (p. 558)

20574 — 13 février 1997 — **M. Jean-Louis Carrère** souhaite appeler l'attention de **Monsieur le garde des Sceaux, ministre de la Justice,** sur les inquiétudes de bon nombre de nos concitoyens quant aux perspectives d'une refonte de la loi informatique et liberté de 1987. La presse s'est faite l'écho qu'un rapport en préparation retiendrait parmi ses principales conclusions la diminution des pouvoirs de la Commission nationale de l'informatique et des libertés (CNIL). De telles propositions ne sauraient être débattues en catimini compte tenu de l'importance croissante des fichiers dans la vie quotidienne et de la nécessité concomitante de veiller à ce qu'ils n'attentent pas à la vie privée. En conséquence, il lui demande de bien vouloir lui confirmer l'existence d'un tel rapport ainsi que de lui préciser les objectifs recherchés par le Gouvernement.

Réponse. — Le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire qu'il incombe à la France d'opérer, avant le 24 octobre 1998, la transposition dans son droit interne de la directive n° 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données. Cette échéance a conduite le Gouvernement à demander au Conseil d'État de procéder à une mission d'analyse et d'approfondissement des très nombreux choix d'options que ménage aux États le texte communautaire susvisé. Un rapport, dont les conclusions sont soumises à la concertation interministérielle, sans qu'il préjuge pour autant des choix qui pourront être retenus, a été ainsi remis au garde des Sceaux. Ce document tient compte des différences importantes que présente la directive, par sa philosophie comme par les solutions qu'elle apporte, avec la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Il analyse, à cet égard, les conséquences de la limitation par la directive du champ de contrôle a *priori* des traitements aux seuls fichiers générateurs de risques particuliers et du renforcement qu'elle induit en contrepartie des procédures de contrôles a *posteriori* pour les autres catégories de fichiers. Les perspectives, déterminées par la transposition, d'une évolution des prérogatives de l'autorité de contrôle que constitue la Commission nationale de l'informatique et des libertés tiennent par conséquent à un recentrage de pouvoirs de celle-ci et non pas à leur diminution. Une telle perspective d'évolution est tout état de cause compatible avec l'exigence du maintien, dans le régime issu de la transposition de la directive, d'un niveau de protection et de garanties équivalent à celui qui est présentement assuré par la loi informatique et libertés.

Sénat 3 avril 1997 n°14 (p. 1055)

MARKETING DIRECT

Mineurs

19168 — 5 décembre 1996 — **M. Nicolas About** attire l'attention de **Monsieur le ministre des Petites et Moyennes entreprises, du Commerce et de l'Artisanat** sur les courriers publicitaires adressés aux mineurs. Il lui rappelle l'existence de fichiers publicitaires qu'utilisent les entreprises pour cibler leur clientèle. C'est le cas, par exemple, des entreprises de presse qui se communiquent entre elles le nom de leurs clients pour abreuver leurs boites aux lettres d'offres d'abonnement. Ce procédé commercial bien connu, s'il incommode la plupart de leurs destinataires adultes, devient inadmissible quand les destinataires sont des mineurs. Que des enfants soient des cœurs de cible pour les publicitaires n'est certes pas une nouveauté, mais qu'on aille jusqu'à leur appliquer les mêmes techniques de marketing par correspondance, pour en faire de futurs petits clients, est contraire à toute déontologie commerciale.

Quand on sait combien la lourdeur des démarches pour réclamer l'arrêt des envois publicitaires est dissuasive pour les consommateurs, on ne peut que s'inquiéter devant la généralisation probable de telles pratiques. I lui demande, par conséquent, quelles mesures il entend prendre pour réglementer plus fermement l'exploitation commerciale de ces fichiers publicitaires, et surtout pour interdire qu'y figurent les mineurs. Question transmise à Monsieur le ministre de l'Économie et des Finances.

Réponse. — La constitution de fichiers commerciaux pour la prospection de la clientèle est une nécessité économique pour toute entreprise qui souhaite développer son activité, notamment en matière de vente à distance. Cette pratique doit cependant être exercée dans le respect des dispositions spécifiques prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En ce qui concerne les fichiers commerciaux, une déclaration auprès des services de la Commission nationale de l'informatique et des libertés (CNIL) est obligatoire (art. 16). Pour les fichiers informatisés comportant des données nominatives concernant des mineurs (clubs sportifs, cartes jeunes par exemple), la CNIL peut formuler des observations sur la prospection et l'utilisation de ces données lors de la demande d'avis qui lui est adressée. Par ailleurs, les droits accordés à toute personne par la loi, droit d'accès et de rectification sur les données les concernant faisant l'objet d'un traitement informatisé, peuvent être exercés les responsables légaux, le mineur n'ayant pas la capacité juridique pour le faire. Les parents peuvent donc, conformément à la loi, saisir la CNIL S'agissant de l'évolution générale de cette loi qui encadre la constitution de fichiers informatisés, une directive européenne (9528 CE du 24 octobre 1995) impose désormais aux responsables d'avertir les personnes du fait qu'ils recueillent une information nominative les concernant. Cette

disposition novatrice qui limite le risque de fichage à l'insu des intéressés doit être transposée en droit national au plus tard au 24 octobre 1998.

Enfin, les fichiers étant destinés principalement à faciliter la prospection commerciale à distance, il convient d'assurer la protection des consommateurs en ce domaine. Une nouvelle directive ayant cet objectif vient d'être adoptée, avec le soutien actif de la France, par le Conseil de l'Union européenne et le Parlement européen. Cette directive sur les contrats à distance prévoit que les informations adressées aux consommateurs par une technique de communication à distance doivent respecter autant les principes de protection des mineurs que les principes de loyauté en matière de transactions commerciales.

Sénat 3 avril 1997 n° 14 (p. 1034)

POLICE

Fichier GEVI

1199 — 14 juillet 1997 — **M. Noël Manière** attire l'attention de **Monsieur le ministre de l'Intérieur** sur la situation créée par la décision de la Commission nationale de l'informatique et des libertés (CNIL) d'autoriser les Renseignements Généraux parisiens d'intégrer dans leur nouveau fichier, le GEVI (gestion des violences). « les signes physiques particuliers, objectifs et inaltérables comme éléments de signalement des personnes susceptibles de violences urbaines » (la couleur de la peau étant notamment un de ces signes). De plus, le fichier pourra receler les « activités politiques, philosophiques, religieuses ou syndicales » desdites personnes. Cette autorisation de la CNIL intervient en application d'un décret général du 14 octobre 199-1 sur les fichiers des renseignements généraux qui élargit le domaine de la sûreté de l'État à la sécurité publique qui comprend, outres les violences urbaines, les atteintes à l'ordre public, définition dont on connaît bien les difficultés pratiques d'interprétation. Cette question touchant le domaine sensible des libertés publiques et des droits de la personne, il lui demande, d'une part, s'il ne. serait pas opportun de reporter la publication de l'arrêté portant création du GEVI, tant que ces dispositions n'auront pas été rapportées, d'autre part, s'il ne serait pas justifié de redéfinir le champ d'application du décret général du 14 octobre 1991 sur les fichiers des Renseignements généraux.

Réponse. — Il convient de rappeler à l'honorable parlementaire que le projet de création du fichier « GEVI » s'est inscrit dans le cadre de la restructuration des services des Renseignements généraux de la préfecture de police engagée en 1994 et de la création d'une sous-direction de la violence et du terrorisme, dont la mission consiste à rechercher toute information relative aux violences politiques, aux violences urbaines et au terrorisme. Ce traitement automatisé doit permettre à la direction des Renseignements généraux de la préfecture de police de rapprocher et d'exploiter rapidement les informations doit elle dispose, sur les personnes physiques majeures et les personnes morales, qui peuvent être impliquées dans des actions violentes de nature à porter atteinte à l'ordre public et au fonctionnement des institutions. La Commission nationale de l'informatique et des libertés (CNIL), qui a approuvé la mise en œuvre de ce traitement dans sa délibération du 19 novembre 1996, a motivé son avis en se fondant sur la stricte conformité du projet aux dispositions du décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des Renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi du 6 janvier 1978. La Commission s'est notamment attachée à vérifier que les informations enregistrées dans l'application n'excédaient pas le champ expressément délimité par le texte de 1991.

C'est ainsi que conformément à l'avis de la CNIL, le fichier « GEVI » comporte une rubrique « signalement » entrant parfaitement dans le cadre du décret précité, dont l'article 2-1 ° permet de faire apparaître « les signes particuliers, objectifs et inaltérables.

A cet égard, il est à noter que toutes les possibilités ouvertes par le dispositif réglementaire ne sont pas utilisées par l'application « GEVI ». En effet, alors que la CNIL admet par les termes « signes particuliers objectifs et inaltérables » que pourrait être fichée la couleur des yeux ou celle de la peau « GEVI » ne fait jamais référence à cette dernière mention. D'autre part, en application de l'article 2-2° du même décret, autorisant l'enregistrement des informations relatives aux activités politiques, philosophiques, religieuses ou syndicales, la CNIL a également validé la création d'une rubrique « activités » dans le fichier « GEVI », qui vise plus précisément les activités liées au travail ou à tout autre élément justifiant directement l'attention portée à un individu potentiellement violent. Toutefois, le ministre de l'Intérieur a indiqué par courrier du 11 Juillet dernier au président de la CNIL, qu'il souhaite se donner le temps d'un réexamen du contenu de ce fichier avant toute décision d'utilisation assortie de modifications complémentaires, ou d'arrêt de sa réalisation.

Assemblée nationale 25 août 1997 n° 27 (p. 2725)

Accès *de la gendarmerie aux fichiers*

47985 — 10 février 1997 — **M. Dominique Paillé** demande à **Monsieur le ministre de la Défense** de bien vouloir lui préciser les mesures qu'il envisage de prendre pour faciliter l'interrogation des différents fichiers administratifs : Carte grise, permis de conduire, sécurité sociale, URSSAF, impôts, etc., par les services de gendarmerie afin de favoriser leur travail de recherche et d'enquête.

Réponse. — Les principes qui gouvernent l'accès aux fichiers informatisés sont réglementés par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans ce cadre, les traitements automatisés d'informations nominatives appliqués dans le secteur public sont soumis au régime de l'autorisation préalable, donnée principalement par un acte réglementaire ou, dans des cas particuliers, par la loi. Tout acte réglementaire portant création d'un traitement automatisé d'informations nominatives doit désigner de manière exhaustive, à l'organisme déclarant, les destinataires internes ou externes qui pourront accéder aux données figurant dans le traitement. Ainsi, la Gendarmerie nationale est habilitée à consulter, par le réseau téléphonique commuté, les informations portées dans le fichiers des déclarations préalables à l'embauche. Elle peut également accéder directement au système national des permis de conduire depuis le 14 novembre 1995 et au fichier national des automobiles depuis le 15 décembre 1995, en utilisant les 11 000 terminaux de son réseau de messagerie. Par ailleurs, la finalité déclarée de certains fichiers informatiques, comme ceux de la Sécurité sociale ou des impôts, ne justifie pas de rendre la gendarmerie directement destinataire des informations nominatives y figurant. Dans ce cas, leur accès est toutefois autorisé aux officiers de police judiciaire de la gendarmerie agissant sur commission rogatoire dans le cadre d'une information judiciaire.

Assemblée nationale 24 mars 1997 n° 12 (p. 1531)

Fichiers des détenteurs d'armes à feu

1709 — 24 juillet 1997 — **M. Bernard Plasait** appelle l'attention de **Monsieur le ministre de l'Intérieur** sur l'inquiétude que soulève chez les citoyens le développement des fichiers des armes soumises à déclaration. Les acquisitions d'armes sont déjà soumises à l'inscription sur les registres de police tenus par les commerçants sous le contrôle des services de police. Elles donnent lieu également à inscriptions sur les

registres en place dans les préfectures, autrefois réservés aux armes les plus dangereuses et aujourd'hui à la quasi-totalité de celles détenues. Ce dispositif débordant sera prochainement encore prolongé par un fichier national des armes, dont l'utilisation potentielle est à l'expérience incontrôlable. Si les armes les plus dangereuses (dites de première et de quatrième catégories relevant du régime de l'autorisation) doivent être légitimement soumises à de telles règles, l'extension prise par les fichiers relatifs aux déclarations devient inquiétante pour les citoyens soucieux de préserver leur vie privée. Il faut également souligner que de tels fichiers pourraient être détournés à des fins malveillantes, les adresses des détenteurs d'armes pouvant se trouver entre des mains mal intentionnées. De surcroît, l'administration préfectorale n'est plus en mesure de contrôler les demandes déposées et de tenir à jour les fichiers en cause, qui comportent des dizaine de milliers de documents, ce que démontrent les reports successifs des délais (de 1996 à 1999) pour l'application du décret du 6 mai 1995. Il lui demande donc de bien vouloir lui indiquer les mesures qu'il entend prendre, dans un souci de préservation de la vie des citoyens, d'une meilleure administration et de relations plus confiantes avec les usagers, afin de parvenir à une application plus paisible de la réglementation en la matière.

Réponse. — L'honorable parlementaire fait état des inquiétudes auprès du ministre de l'Intérieur à l'occasion du projet du fichier national des armes de première et de quatrième catégories qui sera mis en place en 1998 dans les préfectures. Ces armes, comme le souligne l'honorable parlementaire, sont par définition des armes dangereuses et *c'est* la raison pour laquelle les autorisations sont soumises à une durée limitée dans le temps (trois ou cinq ans). Par ailleurs, et sauf exceptions, le nombre d'armes autorisées par individu est limité à une seule. Dans ces conditions, il est nécessaire pour les services préfectoraux non seulement d'être en mesure d'assurer la gestion et le suivi de la délivrance de ces autorisations, mais également de contrôler vigoureusement les conditions dans lesquelles ces autorisations sont données. Le projet de création d'un fichier national décidé par le Gouvernement en fin d'année 1996 a donc pour objectif non pas la création ex *nihilo* d'un fichier nouveau, mais le rassemblement sous forme rationnelle de l'ensemble des données collectées, département par département. Il va sans dire que lorsque le principe de conception de ce futur fichier national aura été établi, il sera présenté et soumis préalablement à l'approbation de la Commission nationale de l'informatique et des libertés.

Il convient également de préciser que ce fichier national est rendu nécessaire par l*a* mise en application de *la* directive du Conseil du 18 juin 1991, laquelle, dans son article 13, oblige les États membres à créer un réseau d'échange d'informations pour assurer la gestion des transferts d'armes entre les États de l'Union. C'est la raison pour laquelle le décret n° 95-589 du 6 mai 1995 a repris dans un article 46-1er alinéa l'obligation pour les préfectures de dresser un fichier des détenteurs de matériels, armes et munitions des première et quatrième catégories. Ce fichier, comme l'ensemble des autres fichiers gérés par les préfectures (notamment le fichier des cartes grises, des passeports, des cartes d'identité...), sera conçu dès le départ afin d'éviter toute manipulation ou tout détournement de données à des fins malveillantes. C'est ainsi que les droits d'accès au quotidien par les agents publics seront très précisément définis, que les agents habilités recevront une formation spécifique et qu'enfin les droits de consultation seront limitativement attribués à certains fonctionnaires. De surcroît, ce type de fichier est de par sa nature un fichier à caractère administratif et les consultations éventuelles par les services de police le seront dans le cadre d'un protocole afin d'une part d'encadrer les informations communicables et d'autre part de fixer les règles pour lesquelles les interrogatoires seront autorisés. La construction de ce fichier se fera selon les normes techniques en vigueur et de ce fait bénéficiera, comme l'ensemble des autres fichiers gérés par le ministère de l'Intérieur, du maximum de sécurité tant pour éviter les intrusions malveillantes que pour

assurer tout au long de la chaîne du traitement de l'information la protection de la vie privée des citoyens.

Sénat 4 septembre 1997 n° 33 (p. 2297)

SANTÉ

Secret et société de l'informations

1229 — 10 juillet 1997 — **M. Emmanuel Hamel** attire l'attention de **Monsieur le secrétaire d'État à la Santé** sur le vœu exprimé dans le seizième rapport annuel d'activité de la Commission nationale de l'informatique et des libertés (CNIL), rendu public le 8 juillet 1996 est rapporté par le *Bulletin Quotidien* du 9 juillet 1996, pages 21 et 22 que « les réseaux qui vont être développés entre les établissements de soins, les professionnels de santé (médecins, pharmaciens) et les organismes de protection sociale ne facilitent pas la divulgation et le détournement des données médicales ». Il lui demande quelle est sa réaction face à ce vœu et quelles mesures il envisage pour maintenir, en tenant compte des nouvelles techniques, le secret médical. Question transmise à Madame le ministre de l'Emploi et de la Solidarité.

Réponse. — Les réseaux évoqués par l'honorable parlementaire sont développés dans le cadre des systèmes d'information en santé.

Pour pouvoir fonctionner, les réseaux de soins, entendus au sens des ordonnances n° 96-345 du 24 avril 1996 auront besoin de ces réseaux de communication. A terme, c'est tout le système de santé qui sera concerné, puisque le nouvel article L. 161-29 du code de la Sécurité sociale prévoit la communication par feuille de soins électronique aux organismes d'assurance maladie du « numéro de code des actes effectués, des prestations servies... et des pathologies diagnostiquées » par les professionnels et les organismes dispensant des actes ou des prestations remboursables. De plus, l'article L162-1-6 prévoit le portage du carnet de santé sur le volet de santé de la carte de bénéficiaire de l'assurance maladie. Toutes ces opérations de transfert, soit de données médicales (texte ou images) soit de la feuille de soins électronique, nécessitent un réseau télématique sécurisé qui garantisse confidentialité et secret médical. C'est pourquoi l'État et les organismes d'assurance maladie ont fait le choix de mettre en œuvre un réseau télématique de type intranet portant le nom de « Réseau Santé Social » (RSS). Un appel d'offres vient d'être lancé par le Gouvernement pour la création de ce réseau. Celui-ci bénéficiera d'une concession de service public. L'accès au réseau ne sera possible qu'avec la carte de professionnel de santé (CPS, prévue par l'article L. 161-33 du code de la sécurité sociale) qui sera diffusée à l'ensemble des professionnels sous le contrôle des directions départementales des affaires sanitaires et sociales. La saisie de la feuille électronique de sécurité sociale nécessitera l'usage simultané de la carte de bénéficiaire de l'assurance maladie (SESAM-VITAL). La CPS permettra également la lecture ou l'écriture d'informations sur le volet de santé de la carte, sélectionnant, en fonction de la profession exercée, les informations accessibles aux différents professionnels. Les données seront toutes chiffrées sur le postes du professionnel de santé avant d'être transmises sur le réseau et déchiffrées sur le poste de receveur.

Ainsi, le Gouvernement, tout à fait conscient de la nécessité de préserver la confidentialité des données qui circuleront sur le réseau santé social, en a fait l'enjeu majeur de son appel d'offres, les autres aspects technologiques soulevant nettement moins de problèmes. Mais les solutions ne sont pas seulement d'ordre technique. Au niveau collectif, la mise en place des fichiers devra se conformer aux prescriptions de la loi sur l'informatique et les libertés. Sur le plan individuel, un rappel régulier à tous les professionnels concernés de leurs obligations en matière de secret professionnel sera

nécessaire. Enfin, il sera indispensable d'informer les usagers de leurs droits, ainsi que des devoirs des professionnels à leur égard, de façon qu'ils puissent eux-mêmes exercer leur vigilance.

Sénat 13 novembre 1997 n° 43 (p. 3159)

TÉLÉCOMMUNICATIONS

Identification de l'appelant

3690 — 29 septembre 1997 — **M. Olivier de Chazeaux** souhaite appeler l'attention de **Monsieur le secrétaire d'Etat à l'Industrie** sur les nouveaux services de France Télécom en matière d'identification d'appels téléphoniques. En effet, il est désormais possible aux détenteurs de postes prévus à cet effet de connaître le numéro de téléphone de leur correspondant lorsque ce dernier appelle. Les avantages affichés par l'opérateur public sont certains : Lever l'inconnu entourant l'appel et détourner les gêneurs. Un problème subsiste toutefois concernant les abonnés inscrits sur liste rouge.

Par définition, leur numéro de téléphone doit rester confidentiel.

Or ce même numéro apparaît sur tous les postes équipés du signal d'identification. L'anonymat n'est garanti par France Télécom que sur demande de l'abonné. On comprend dès lors l'absurdité d'une situation où l'abonné sur liste rouge doit faire une démarche pour être anonyme lorsqu'il appelle. Dans ces conditions il lui demande de veiller au respect de l'anonymat des personnes inscrites sur liste rouge, et plus généralement, lui demande les moyens qu'il compte mettre en oeuvre pour que l'anonymat soit garanti lorsque la dérégulation du secteur des télécommunications, prévue pour 1998, sera effective.

Réponse. — la présentation du numéro est un service qui rencontre un grand succès dans de nombreux pays autres que la France et que France Télécom a soigneusement testé avant de le mettre sur le marché. Les expérimentations en vraie grandeur ont révélé qu'une majorité de clients inscrits en liste rouge préférait, pour ne pas dévoiler leur numéro en appelant un correspondant, la possibilité de secret appel par appel à celle de secret permanent, pour des raisons de souplesse d'utilisation. Compte tenu du résultat de ces tests, France Télécom a décidé, en concertation avec la Commission nationale de l'informatique et des libertés, de proposer à l'ensemble de ses clients ce service et les deux possibilités de restriction pour ceux qui s'opposent à la communication de leur numéro. Une très large campagne d'information, définie avec la CNIL, a été mise en œuvre dès le 28 mai 1997, par voie de presse et par *mailing,* afin de donner à tous les clients le temps de faire leur choix. Tous les clients ont reçu *La Lettre de France Télécom* de juin — juillet, présentant le service et les possibilités de secret.

Ainsi, ils ont été informés des deux possibilités qui leur sont offertes gratuitement pour préserver la confidentialité de leur numéro : Soit en utilisant le 3651 avant le numéro de son correspondant, soit en optant pour le secret permanent, sur simple demande auprès de leur agence commerciale de France Télécom. Le secret appel par appel et le secret permanent sont gratuits. De plus, les abonnés liste rouge ont reçu un publipostage personnalisé consacré exclusivement à ce nouveau service. Ces deux options garantissent l'anonymat des clients, systématiquement ou non selon leur désir. En 1998, France Télécom continuera à respecter le choix fait par ses clients de présenter ou non leur numéro.

Assemblée nationale 24 novembre 1997 n° 40 (p. 4251)

TRAVAIL

Surveillance des salariés

19835 — 2 janvier 1997 — **M. Emmanuel Hamel** attire l'attention de **Monsieur le ministre du Travail et des Affaires sociales** sur la constatation faite dans le seizième rapport annuel d'activité de la Commission nationale de l'informatique et des libertés (CNIL) rendu public le 8 juillet dernier et rapporté par le *Bulletin quotidien* du 9 juillet dernier (pages 21 et 22) que « l'informatique est en train d'investir le cœur même de la relation de travail en constituant un encadrement imperceptible mais réel qui s'ajoute ou se substitue au contrôle humain. Le risque réside dans la multitude des instruments de collecte et de traitement de données qui permettent de saisir, au-delà de tel ou tel acte, un comportement ou une personnalité dans sa globalité ». Il lui demande quelle est sa réaction face à cette constatation et s'il envisage de prendre des mesures pour prévenir ce risque engendré par le développement des nouvelles technologies informatiques et notamment le télé-travail.

Réponse. — Le ministre du Travail et des Affaires sociales estime préoccupants les risques que comporte à l'égard des droits des personnes le développements dans les entreprises des nouvelles technologies informatiques. Cependant, la législation française encadrant l'utilisation de ces technologies dans les relations de travail peut apparaître, à bien des égards, exemplaire. En effet, l'utilisation des technologies de l'information dans les relations de travail est encadrée, d'une part par la loi du 6 janvier 1978 qui protège les données personnelles et, d'autre part, par la loi du 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage dont le titre V est consacré au recrutement et aux libertés individuelles dans l'entreprise. Ainsi, l'article L. 120-2 du code du travail pose comme principe que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. Par ailleurs, l'article L. 121 -8 du code du travail dispose qu'aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collecté par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat. Le comité d'entreprise doit également être informé et consulté préalablement à l'installation d'un système permettant un contrôle de l'activité des salariés (art. L. 432-2-1 du code du travail). De plus, l'article L. 422-1-1 du code du travail permet au délégué du personnel qui constate une atteinte aux libertés individuelles dans l'entreprise, qui ne serait pas justifié par la nature de la tâche à accomplir ni proportionnée au but recherché, de saisir l'employeur afin que celui-ci ne prenne les dispositions nécessaires. Le non-respect par l'employeur de ces obligations pourrait conduire les juges à ordonner le retrait du matériel utilisé. Par ailleurs, les dispositions du code du travail en matière de durée du travail sont d'ordre public et doivent s'appliquer en tout état de cause, quelles que soient les techniques utilisées, de même que les dispositions plus favorables des conventions ou accords collectifs dans ce domaine. Ainsi, en matière d'horaires de travail, le décret du 18 décembre 1993 a redéfini les obligations incombant aux employeurs en vue de permettre le contrôle de la durée du travail. Ce texte rappelle les dispositions antérieurement applicables aux salariés occupés en horaire collectif (affichage sur les lieux de travail, transmission à l'inspection du travail). Il crée, par ailleurs, l'obligation d'établir un décompte quotidien, ainsi qu'une récapitulation hebdomadaire des heures de travail pour tout salarié occupé en horaire non collectif.

Les appels professionnels par téléphone portable peuvent, le cas échéant, être justifiés s'ils répondent à une nécessité de l'entreprise. Les inventions professionnelles que le salarié serait amené à faire à la suite de ces appels devront être décomptés comme temps de travail effectif, dans les conditions identiques à une astreinte. Toutefois tout abus

de l'employeur concernant le nombre et le moment de ces appels, notamment en tous lieux et à toutes heures, pourrait tomber sur le coup de l'article L. 120-2 du code du travail précité et constituer une atteinte volontaire à l'intimité d'autrui, fait sanctionné par l'article L. 226-1 du nouveau code pénal. Enfin les juridictions n'hésitent pas à récuser, comme mode de preuve illicite, tout moyen utilisé à l'insu des salariés. Ainsi, la chambre sociale de la Cour de cassation, dans un arrêt du 22 mai 1995, a jugé sans cause réelle et sérieuse le licenciement d'un agent commercial fondé sur les rapports d'un détective privé chargé de suivre le salarié dans ses déplacements professionnels, l'employeur ne pouvant contrôler l'activité de ses employés au moyen d'un dispositif n'a pas été porté à leur connaissance. Dans un autre arrêt du 7 juin 1995, la Cour suprême conclut à la faute de l'employeur qui avait institué un nouveau système de paie informatisé avant d'en avoir fait la déclaration à la CNIL, et reconnaît aux salariés le droit à des dommage et intérêts en réparation du préjudice subi par le défaut d'information préalable. L'ensemble de *ces* dispositions apparaît donc de nature à la fois à prévenir les risques engendrés par l'utilisation de nouvelles technologies et à sanctionner les abus qui peuvent en résulter. Il appartient aux chefs d'entreprise et aux institutions représentatives du personnel de veiller particulièrement, chacun en ce qui les concerne, à leur application.

Sénat 10 avril 1997 n° 15 (p. 1136)

2e RAPPORT D'ACTIVITÉ DE L'AUTORITÉ DE CONTRÔLE COMMUNE DE SCHENGEN

MARS 1997 À MARS 1998

Appendice

PREFACE

La période couverte par le 2e rapport annuel de l'autorité de contrôle commune Schengen (mars 1997 — mars 1998) coïncide avec un moment décisif, d'une importance cruciale pour la coopération policière et pour le Système d'information Schengen à l'échelle européenne : l'élargissement à de nouveaux pays des conditions d'exercice de la liberté de circulation des citoyens, le renforcement du système commun de sécurité et d'information policière et l'intégration de Schengen à l'Union européenne.

1997 a vu s'affirmer l'indépendance et confirmer l'importance de l'autorité de contrôle commune (ACC) en tant qu'organe chargé de veiller au respect des droits et libertés des citoyens et, en particulier, à la protection des données à caractère personnel.

L'ACC est intervenue dans des domaines fondamentaux, contribuant ainsi à ce que, dans son fonctionnement, le Système d'information Schengen respecte les droits et les règles prévus par la Convention d'application. Ainsi elle a analysé les lois grecque et italienne relatives à la protection des données à caractère personnel et a formulé des recommandations et avis sur les conditions de sécurité du traitement et de la transmission des données à caractère personnel, sur la durée de conservation des données, sur les signalements correspondant à des identités usurpées et sur la transmission de certaines données à Interpol.

Les instances exécutives de Schengen ont reconnu l'importance du rôle de l'ACC, qui s'est vu octroyer une ligne budgétaire autonome, transmettre de manière plus régulière les informations indispensables à l'exercice de ses missions et a été consultée dans plusieurs domaines. Les présidences successives

de Schengen (le Portugal, l'Autriche et la Belgique) ont accordé une importance croissante à l'ACC.

Conformément à notre programme de travail, nous avons franchi cette année une étape importante vers la transparence dans le fonctionnement du système et l'information des citoyens. L'ACC a rendu public son dernier rapport lors d'une conférence de presse à Lisbonne, en avril 1997, et l'a transmis aux instances de l'Union européenne et de Schengen ; les commissions nationales l'ont présenté à leurs parlements respectifs ; ce rapport a fait l'objet de plusieurs publications et est disponible sur les pages Internet de plusieurs commissions de protection des données. Lorsque cela s'est justifié, l'ACC n'a pas manqué d'attirer l'attention des instances compétentes et de l'opinion publique sur les problèmes de sécurité qui se sont posés à la suite d'une fuite d'informations dans l'un des bureaux SIRENE. Parallèlement, elle a décidé de lancer, en coopération avec les organes nationaux compétents, une campagne d'information sur les droits des citoyens, face au Système d'information Schengen.

Dans le cadre de l'évolution des systèmes d'information policière européens (Europol, Eurodac, système douanier) et du renforcement des mesures de coopération destinées à la lutte contre la grande criminalité organisée, il importe de développer les mécanismes de coopération entre les Autorités de contrôle communes chargées, dans chacun de ces systèmes, de la sauvegarde des valeurs fondamentales de la liberté et de la citoyenneté. L'ACC cherchera à promouvoir cette coopération et continuera de compter sur le soutien actif des commissions nationales de protection des données à caractère personnel.

Prévue par le traité d'Amsterdam, l'intégration de Schengen à l'Union européenne permettra d'en accroître la transparence. La législation européenne sera enrichie par les règles relatives à la protection des données personnelles prévues par la Convention d'application de Schengen. L'acquis Schengen qui sera intégré à l'Union reprendra également les recommandations les plus importantes de l'ACC en la matière et déterminera le rôle qu'elle sera appelée à jouer.

C'est dans le but de la réalisation d'un espace européen commun de liberté dans la sécurité que l'ACC planifiera ses missions et déploiera tous ses efforts.

Le 26 février 1998

Le président, Joao
Labescat

Chapitre I

INTRODUCTION

Dans son premier rapport d''activité, l'autorité de contrôle commune a rappelé les étapes franchies par les cinq États signataires de l'accord de Schengen depuis 1985, jusqu'à la signature de la Convention d'application de cet accord en 1990, et plus tard, en mars 1995, la mise en application de cet instrument. Elle a aussi montré comment, au cours de cette période, les cinq pays signataires ont été rejoints par dix autres, désireux eux aussi de faire partie de cet espace de libre circulation des personnes [1].

Elle a également décrit les mesures compensatoires prévues par la Convention d'application de l'accord de Schengen afin de permettre la réalisation de son objectif, la suppression des contrôles aux frontières intérieures des États membres, et, partant, la création d'un grand espace de libre circulation des personnes, tout en maintenant à l'intérieur de celui-ci un niveau de sécurité au moins égal à celui qui existait auparavant. Un bref rappel de ces mesures figure ci-après.

Parmi les mesures compensatoires à la suppression des contrôles aux frontières intérieures prévue par la Convention figure, à côté d'une harmonisation de la politique de délivrance des visas, d'une politique commune sur la détermination de l'État responsable du traitement de la demande d'asile, d'une amélioration de la coopération policière et judiciaire, d'une intensification de la lutte contre le trafic illicite de stupéfiants, ou de l'harmonisation du niveau de contrôle aux frontières extérieures du territoire Schengen, un Système informatique Schengen (SIS).

[1] Les États suivants sont membres de l'ACC Allemagne, Autriche, Belgique, Espagne, France, Grèce, Italie. Luxembourg, Pays-Bas, Portugal. Les cinq Etats nordiques (Danemark, Finlande, Islande, Norvège, Suède) participent aux travaux de l'ACC en tant qu'observateurs.

Celui-ci relie l'ensemble des pays appliquant la Convention d'application de l'accord de Schengen, et permet à ses utilisateurs (services chargés de missions de police, ambassades et consulats, etc.) de disposer en temps réel des informations utiles à leurs missions, introduites par n'importe quel État membre appliquant la Convention.

Ces informations ont trait à des personnes (recherchées pour arrestation aux fins d'extradition, non admises, disparues, devant faire l'objet d'une surveillance discrète,...), et à des biens (véhicules, armes, documents, billets de banque volés, détournés, ou égarés). La création d'un tel instrument s'est accompagnée de celle d'une autorité de contrôle commune à la protection des données à caractère personnel (ACC), chargée notamment de veiller au respect des dispositions de la Convention à l'égard de la fonction de support technique du SIS (article 115). Un rôle de conseil et d'harmonisation des pratiques ou des doctrines nationales est également confié à cet organe composé de deux représentants de chacune des autorités de contrôle des parties contractantes.

L'ACC a eu fort à faire depuis la mise en application de la Convention, pour faire reconnaître ses compétences et son indépendance vis-à-vis des organes exécutifs de Schengen. Son premier rapport d'activité l'a montré, notamment en soulignant les difficultés rencontrées pour obtenir un budget autonome, ou celles rencontrées par le groupe d'experts désignés par l'ACC pour contrôler la partie centrale du SIS (C.SIS), installée à Strasbourg.

A la date d'approbation du présent rapport, plus d'un an après le contrôle du C.SIS, l'ACC n'a toujours pas reçu de réponse des instances exécutives de Schengen aux recommandations formulées à la suite du contrôle du C.SIS, mais seulement du ministère de l'intérieur français. Quant aux informations relatives au C.SIS, nécessaires à l'exercice de ses missions, ce n'est qu'en février 1998 que l'ACC en a reçu une partie.

Si des progrès ont été réalisés, il reste beaucoup à faire. La visite de contrôle de l'ACC au C.SIS en 1996 a montré un bon fonctionnement global du système, mais a mis en exergue différents problèmes, dont certains posent de véritables difficultés en termes d'intégrité.

Les problèmes relevés par l'ACC prennent une signification toute particulière alors que le nombre d'États Schengen appliquant la Convention vient d'augmenter, pour passer à la fin de l'année 1997, de 7 à 10. En effet, le nombre de données introduites dans le SIS augmente en conséquence.

Les systèmes d'information policiers évoluent, y compris celui de Schengen. Cette évolution doit s'accompagner d'une augmentation du rôle des autorités de contrôle indépendantes concernées. L'intégration de Schengen dans l'Union européenne, prévue par le traité d'Amsterdam, à l'article 7 du protocole intégrant l'acquis de Schengen, signifie plus de transparence et de garanties pour les droits fondamentaux des citoyens. Les parlements nationaux et les instances européennes prendront une part active à la réalisation de ces objectifs.

L'AUTORITE DE CONTRÔLE COMMUNE ET SES MISSIONS

Si la mission principale de l'ACC est de contrôler la fonction de support technique du SIS, mission qu'elle a seule le pouvoir d'accomplir (article 115.2), un rôle de conseil et d'harmonisation des pratiques ou des doctrines nationales lui est également confié.

La Convention d'application de l'accord de Schengen précise ses missions à l'égard du SIS dans les articles suivants :

ARTICLE 106.3

L'ACC rend un avis en cas de désaccord entre deux parties sur l'existence d'une erreur de droit ou de fait entachant un signalement. Il s'agit d'un cas obligatoire de saisine par la partie qui n'est pas à l'origine du signalement.

ARTICLE 115.3

L'ACC analyse les difficultés d'application ou d'interprétation pouvant survenir lors de l'exploitation du SIS.

L'ACC étudie les problèmes pouvant se poser lors de l'exercice du contrôle indépendant effectué par les autorités de contrôle nationales des parties contractantes.

L'ACC étudie les problèmes pouvant se poser à l'occasion de l'exercice du droit d'accès au système.

De manière plus générale, l'ACC élabore des propositions harmonisées en vue de trouver des solutions aux problèmes existants.

ARTICLE 115.4

L'ACC établit des rapports qui sont transmis aux instances auxquelles les autorités de contrôle nationales transmettent leurs rapports.

ARTICLE 118.2

L'ACC reçoit communication des mesures particulières prises par chaque partie contractante en vue d'assurer la protection des données lors de la transmission de données à des services situés en dehors des territoires des parties contractantes.

S'agissant des échanges d'informations hors SIS :

ARTICLE 126.3. F)

L'ACC peut, à la demande des parties contractantes, émettre un avis sur les difficultés d'application et d'interprétation de l'article 126 relatif au traitement des données transmises, hors SIS, en application de la Convention.

ARTICLE 127.1

L'ACC peut, dans les conditions et selon les modalités prévues par l'article 126, émettre un avis en cas de transmission de données provenant d'un fichier non automatisé et d'intégration de données dans un tel fichier.

Chapitre III

L'ACTIVITE DE L'AUTORITÉ DE CONTRÔLE COMMUNE DE MARS 1997 À MARS 1998

De mars 1997 à mars 1998, l'ACC s'est réunie en composition plénière à dix reprises. A l'exception de la session annuelle tenue par l'ACC à Lisbonne en avril 1997, à laquelle le représentant du président du Comité exécutif a pris part, ces réunions se sont tenues à Bruxelles.

Outre ces réunions plénières, l'ACC a tenu cinq réunions restreintes, afin de préparer des projets d'« avis » sur des problèmes particuliers, rédiger son rapport annuel, et examiner les futures modalités du contrôle du C.SIS. Par ailleurs, à trois reprises, plusieurs de ses membres ont rencontré des représentants du ministère de l'intérieur français, en tant que responsable de la fonction de support technique du C.SIS. Lors d'une de ces rencontres, une troïka des présidences Schengen était présente, afin notamment de faire le point sur le suivi des recommandations émises par l'ACC à l'issue de son contrôle du C.SIS.

Il est à noter que, depuis la réunion de l'ACC du 7 mars 1997, conformément à la décision prise au sein de cette autorité lors de sa réunion des 10 et 11 février 1997 à Strasbourg, la Suède, le Danemark, la Finlande, la Norvège et l'Islande prennent part aux réunions de l'ACC en tant qu'observateurs.

Au cours de ces réunions, les questions suivantes ont été examinées :

LE FONCTIONNEMENT DE L'ACC

La composition de l'ACC

L'ACC a pris acte de l'existence des lois italienne et grecque réglementant la protection des données à caractère personnel. Il s'agit là d'une des conditions préalables au chargement de données à caractère personnel dans le SIS (article 117), et donc, à la mise en application de la Convention sur le territoire des États membres.

L'ACC a adapté son règlement intérieur [1], afin de pouvoir attribuer le statut de membres de l'ACC aux représentants d'autorités nationales de contrôle d'États ayant adhéré à la Convention dès que, toutes les autres conditions étant remplies, la Convention est mise en application sur leur territoire.

Sur la base de ce critère, il a été constaté, lors de la réunion de l'ACC du 12 décembre 1997, que les représentants des autorités de contrôle de l'Italie, l'Autriche et la Grèce participent désormais aux réunions de l'ACC en qualité de membres de celle-ci.

L'élection du président et du vice-président

L'ACC a élu, le 12 décembre 1997, M. J. Labescat (Portugal) en tant que président, et M. B. De Schutter (Belgique), le 3 février 1998, en tant que vice-président.

La ligne budgétaire autonome de l'ACC

Le budget de l'ACC pour l'année 1997 a, au terme de longues discussions de principe, été approuvé par les autorités Schengen.

La version approuvée par le Comité exécutif le 25 avril 1997 a ensuite été adaptée à l'augmentation du nombre de pays représentés à ses réunions. Le budget alloué à l'ACC pour l'année 1997 s'élevait à 2 839 950 FB. Le 12 décembre 1997, l'ACC a procédé à la clôture des comptes de son budget 1997. Les comptes ont fait apparaître un solde de 992 179 FB, sur le budget de 2 839 950 FB qui lui avait été accordé.

Les dépenses de l'année ont porté sur la réalisation du fascicule sur le droit d'accès, la rédaction, la traduction et l'impression du premier rapport d'activité, l'organisation de la session annuelle de l'ACC à Lisbonne, et l'achat de divers biens d'équipement. Le budget 1998, basé sur les dépenses 1997 et tenant compte du programme d'activités de l'ACC pour l'année 1998, a été approuvé le 23 février 1998 par le groupe central. Ce budget s'élève à 3 239 950 FB.

[1] Ce document figure en annexe au présent rapport.

Secrétariat de l'ACC

A plusieurs reprises, l'ACC a demandé un renforcement des moyens logistiques mis à sa disposition, ainsi qu'une priorité dans les traductions par rapport aux groupes de travail.

Elle a également demandé que la possibilité de disposer d'un secrétariat autonome soit examinée. Trop souvent en effet, le nombre croissant de réunions des groupes de travail Schengen porte atteinte à la préparation de ses propres réunions.

Par ailleurs, l'ACC a constaté que le personnel du secrétariat général était affecté en priorité à la préparation des réunions du groupe central ou du Comité exécutif. Ce problème a été partiellement résolu par l'attribution d'un budget à l'ACC, couvrant notamment les frais de traduction de son rapport annuel. Le 23 février 1998, le groupe central a marqué son accord sur le renforcement du soutien administratif mis à sa disposition.

L'ACC s'en réjouit car elle est d'avis qu'elle ne peut faire face à l'augmentation de ses travaux qu'avec le soutien d'un secrétariat permanent, ou du moins, affecté en priorité à ses travaux.

Elle considère également que le secrétariat actuel, qui a accompagné ses travaux depuis la rédaction de la Convention, est le plus à même de lui apporter ce soutien.

LES SUJETS TRAITÉS PAR L'ACC

Les avis de l'ACC

L'ACC a adopté plusieurs avis, repris ci-après sous le chapitre IV.

Le contrôle du C.SIS

La version finale du rapport technique confidentiel sur le contrôle du C.SIS, effectué en octobre 1996, comprenant les observations du ministère de l'intérieur français, a été approuvée.

Une version provisoire de ce rapport avait été transmise au président du groupe central en décembre 1996, tandis que la version finale a été transmise le 22 avril 1997 au président du Comité exécutif et du groupe central pour diffusion aux groupes techniques compétents.

Ceux-ci ont été chargés de vérifier dans quelle mesure les recommandations formulées par l'ACC afin de sécuriser le système pouvaient être suivies. Presque deux ans après le contrôle, les instances officielles Schengen n'ont toujours pas fait connaître à l'ACC les suites qu'ils entendent donner à ces recommandations.

Les modalités des contrôles du C.SIS par l'ACC

Le protocole visant à préciser les modalités selon lesquelles s'effectueraient à l'avenir les contrôles du C.SIS, a été examiné au cours de l'année.

La plupart des membres de l'ACC ayant estimé, lors de leur réunion du 12 décembre 1997, que le projet auquel avaient abouti plusieurs rencontres entre des représentants du ministère de l'intérieur français et de l'ACC méconnaissait le caractère indépendant de leur institution, il a été décidé qu'une commission restreinte reprendrait l'examen de cette question délicate, afin de proposer un nouveau projet, conciliant les exigences de sécurité posées par le ministère de l'intérieur français et la nécessité de permettre à l'ACC d'exercer ses contrôles en toute indépendance.

Un nouveau projet a été élaboré par un groupe restreint de membres de l'ACC le 2 février 1998, pour être approuvé lors de la réunion plénière du 6 mars 1998. Il servira de nouvelle base aux discussions avec les responsables concernés.

La sécurité des bureaux SIRENE

A la suite de la découverte d'un trafic d'informations sensibles, notamment issues du SIS, en provenance du bureau SIRENE belge [1], l'ACC, directement informée de cet incident, a adopté, lors de sa réunion du 12 décembre 1997, un communiqué de presse. Il a été diffusé le jour même aux agences de presse, et remis le 15 décembre 1997 aux représentants du Comité exécutif.

Dans son communiqué, l'ACC exprimait sa vive inquiétude devant un événement qui met en évidence de manière dramatique la nécessité d'améliorer continuellement les mesures de sécurité dans le cadre du SIS et de l'échange d'informations Schengen.

Elle a invité sans délai les autorités de contrôle nationales à :
lui faire un rapport sur la situation en matière de sécurité en ce qui concerne leur SIS et leur bureau SIRENE ;
définir, sur la base de ces informations, les mesures qui devraient être prises afin d'améliorer la sécurité ;
apprécier la nécessité d'élaborer un rapport annuel sur la situation en matière de sécurité ;
revenir sur ce sujet lors de sa prochaine réunion.

Elle a également souligné qu'il était important qu'elle soit informée à tout moment des mesures de sécurité prises par les instances Schengen et les autorités nationales en vue de garantir la confidentialité du système Schengen.

Depuis cette date, plusieurs autorités de contrôle nationales ont procédé à des vérifications. Les premiers rapports nationaux sont en cours d'examen.

1 Une explication sur la fonction de ces bureaux figure en annexe.

Le rapport d'activité

L'ACC a élaboré son premier rapport d'activité : le 7 mars 1997, un premier projet a été examiné par les membres, pour être approuvé le 27 mars 1997.

La structure du deuxième rapport d'activité de l'ACC a été approuvée le 3 février 1998. Un projet de texte a été discuté le 25 février 1998 par un groupe restreint de rédaction, et à nouveau examiné par l'ensemble des membres de l'ACC lors de leur réunion du 6 mars 1998. Il a ensuite été approuvé au terme d'une procédure écrite.

Une session annuelle de l'ACC a été organisée les 22 et 23 avril 1997 à Lisbonne. Le rapport d'activité de l'ACC y a été présenté au représentant du groupe central, ainsi qu'aux journalistes qui ont assisté à la conférence de presse.

De nombreux journalistes portugais — TV, radio, quotidiens principaux et agence de presse portugaise — ainsi que certains journalistes étrangers, notamment de l'agence EFE (Espagne) et de l'agence Reuter (GB) ont assisté à cette conférence de presse. En outre, la réunion de l'ACC et la présentation du rapport ont été relayées dans des publications périodiques.

Les principaux aspects mis en évidence par les organes de communication sociale étaient : la définition des compétences de l'ACC, son rôle dans le cadre des instances Schengen, le fonctionnement du SIS, et plus particulièrement le type de données enregistrées et les modalités d'accès, ainsi que des informations générales sur la Convention d'application de l'accord de Schengen.

Ce rapport a été diffusé par les autorités de contrôle nationales, de la même manière que le sont d'habitude leurs rapports nationaux et notamment, pour certains d'entre eux, sur Internet. Dans certains pays, des conférences de presse ont été tenues pour présenter ce document, et ainsi mieux faire connaître l'ACC par le grand public.

L'information du citoyen

Afin de remplir sa mission d'information à l'égard des citoyens, l'ACC avait décidé de publier un fascicule, destiné au grand public, sur les droits des *citoyens* signalés dans le SIS.

Le 12 décembre 1997, l'ACC a adopté la version définitive du texte explicatif sur le droit d'accès des personnes aux informations les concernant enregistrées dans le SIS, et a retenu le projet présenté par l'une des sociétés de communication auxquelles il avait été fait appel.

Ce texte, annexé au présent rapport, sera diffusé aux points de passage autorisés pour le franchissement des frontières extérieures de Schengen sous la forme de plaquettes d'information. Des panneaux d'affichage informeront les personnes de l'existence de ces fascicules.

L'efficacité de cette initiative dépendra pour beaucoup de la diffusion qui sera assurée de ces documents. Aussi, l'ACC compte-t-elle être appuyée dans cette entreprise par les autorités nationales de contrôle, les instances Schengen et les autorités compétentes des États.

L'information de l'ACC

En avril 1997, sur demande de l'ACC, le groupe central a invité le C.SIS et l'unité de gestion à mettre leurs rapports mensuels à la disposition de l'ACC. Elle considérait en effet qu'il était nécessaire qu'elle dispose de ces documents afin de pouvoir s'assurer du respect des règles de protection des données à caractère personnel.

Le président du groupe central a adressé, le 7 mai 1997, un courrier au président du groupe de travail permanent ainsi qu'au chef de la délégation française, responsable du C.SIS, les invitant à exécuter la décision du groupe central. Les rapports du C.SIS ont depuis régulièrement été transmis à l'ACC, tandis que ceux de l'unité de gestion ne lui ont été fournis qu'à partir du 6 mars 1998.

Les relations entre l'ACC et les instances Schengen

Une réunion entre des représentants de l'ACC et du groupe central, ainsi que du ministère de l'intérieur français, en tant que responsable du support technique C.SIS, s'est tenue à Bruxelles, le 16 juin 1997.

Les représentants de l'ACC ont ainsi été informés de l'état des travaux relatifs au chargement dans le SIS de données réelles pour l'Italie, la Grèce et l'Autriche. Des précisions ont également été données sur la capacité du SIS pour accueillir ces trois nouveaux pays.

La question des suites réservées au rapport confidentiel sur le contrôle du C.SIS a également été abordée, et les participants ont approuvé la proposition du ministère de l'Intérieur français de mettre au point, en concertation avec des représentants de l'ACC, un protocole définissant les modalités des futurs contrôles de l'ACC au C.SIS. Les modalités d'utilisation du budget de l'ACC ont été précisées, et l'avis de l'ACC 97/1 sur la duplication d'une partie des signalements du SIS a été officiellement présenté.

Le principe de rencontres périodiques entre des représentants de l'ACC et du groupe central, éventuellement, en marge de ses réunions, a été accepté. Celles-ci ont ouvert la porte à une meilleure information réciproque de ces autorités.

C'est ainsi que, le 4 mars 1998, à l'invitation de la Présidence belge, une délégation de l'ACC a pris part pour la première fois à une réunion du groupe central, précédée d'une visite du C.SIS.

Cette rencontre a permis un échange mutuel d'informations : l'ACC a présenté son programme de travail, et rappelé les missions qui lui sont dévolues par la Convention, tandis que des explications techniques sur le développement du SIS lui ont été données.

L'ACC et le groupe central ont convenu qu'à l'avenir, ils s'informeraient davantage et coopéreraient plus étroitement. L'ACC aura ainsi la possibilité de suivre certaines phases des travaux relatifs au SIS, et pourra de la sorte s'assurer que ses recommandations sur la sécurité du système, notamment, sont prises en compte pour l'avenir.

Chapitre IV

LES AVIS RENDUS PAR L'AUTORITÉ DE CONTRÔLE COMMUNE

Au cours de leur examen, il est apparu que plusieurs des avis examinés par l'ACC requéraient des compléments d'information. C'est pourquoi certains des avis mentionnés ci-après figuraient déjà parmi les travaux en cours dans premier rapport d'activité. Par ailleurs, les deux premiers avis qui suivent, approuvés en mars 1997, étaient également repris dans le précédent rapport d'activité. Ces avis sont résumés ci-après, et repris en entier en annexe.

Avis du 7 mars 1997 sur le projet pilote du groupe de travail I « police et sécurité », relatif aux véhicules volés (SCH/Aut-cont (97) 22 rév.)

Le groupe central a transmis à l'ACC le 10 février 1997 une demande d'avis émanant du groupe de travail I « police et sécurité » relative à la participation des pays non intégrés dans le SIS à un projet pilote en matière de vol de véhicules.

Après avoir noté que ce projet tendait à permettre aux pays non intégrés dans le SIS d'interroger celui-ci par le biais de leurs officiers de liaison, l'ACC a demandé des informations complémentaires sur la nature des informations échangées et leur mode de transmission.

Ces éléments lui ayant été donnés, l'ACC a, dans un avis rendu le 7 mars 1997, rappelé que :

— les informations relatives à la marque, au type, à la couleur et aux caractéristiques techniques d'un véhicule ne constituaient pas en soi des données à caractère personnel s'il n'y avait pas de lien entre ces informations et le numéro d'immatriculation, le propriétaire ou le conducteur du véhicule ;

- les échanges d'informations policières au départ des fichiers nationaux entre les parties contractantes intégrées au SIS et les autres États où la Convention n'était pas encore appliquée, relevaient, via les mécanismes de la coopération bilatérale ou multilatérale, des législations en matière de protection des données et du contrôle des autorités de contrôle nationales.

S'agissant des informations directement ou indirectement nominatives enregistrées dans le SIS, l'ACC a estimé qu'elles n'étaient pas accessibles et ne pouvaient pas être consultées directement par les autorités des parties contractantes sur le territoire desquelles la Convention n'était pas encore mise en application, conformément aux articles 101 et 126.1 de la Convention.

Cet avis a été transmis au groupe de travail I, qui en a tenu compte dans la réalisation de son projet. D'autres projets pilote, tel celui en préparation sur les stupéfiants, devront également tenir compte de cet avis.

Avis du 7 mars 1997 sur le projet d'accord de coopération concernant le traitement des infractions routières et l'exécution des sanctions pécuniaires y relatives (SCH/Aut-cont (97) 19 rév.)

Le groupe central a transmis à l'ACC le 10 février 1997 une demande d'avis émanant du groupe de travail III « coopération judiciaire » portant sur un projet d'accord sur les infractions routières.

Le texte prévoit d'une part l'accès aux informations et données figurant dans les registres d'immatriculation des parties contractantes et, d'autre part, un système de notification directe et de coopération ainsi que l'exécution effective par chaque État partie des décisions émanant d'une autorité d'une autre partie contractante, sous réserve de certains cas limitant ou excluant l'application d'une sanction pécuniaire.

Ce projet est fondé sur la déclaration commune des ministres et secrétaires d'État du 19 juin 1990 aux termes de laquelle les parties contractantes s'engagent à entamer ou poursuivre des discussions dans divers domaines dont celui des poursuites contre les infractions en matière de circulation routière et l'exécution réciproque des peines d'amendes.

Il constitue un instrument juridique international distinct mais complémentaire de la Convention de Schengen et référence est faite à son titre VI relatif aux règles de protection des données applicables en cas de transmission d'informations non inscrites dans le SIS.

L'ACC, après avoir examiné les dispositions de protection des données prévues par le projet d'accord, a rendu un avis le 27 mars 1997 dans lequel elle demande que les principes suivants soient intégrés ou explicités :
- le droit de toute personne d'exiger la rectification ou l'effacement de données la concernant qui sont entachées d'une erreur de fait ou de droit ;

- le principe de la coopération entre les autorités de contrôle nationales mentionnées à l'article 128.1 en vue de garantir les droits d'accès, de rectifica tion ou d'effacement ;
- la compétence de l'ACC pour émettre des avis sur les aspects communs en matière de protection des données à caractère personnel découlant de l'appli cation de l'accord.

Cet avis a été transmis au groupe de travail III qui a adapté son projet d'avis en conséquence.

Avis 97/1 du 22 mai 1997 sur la duplication d'une partie des signalements du SIS
(SCH/Aut-cont (97) 38 rév.)

L'article 102.2 précise que les données intégrées dans le SIS ne peuvent être dupliquées qu'à des fins techniques, pour autant que cette duplication soit nécessaire pour l'interrogation directe par les autorités nationales habilitées.

L'ACC, sur la demande de la Commission de la vie privée belge, a engagé, au regard de cet article, une discussion sur l'interprétation de la notion de duplication de données à des fins techniques et sur celle d'interrogation directe notamment par rapport au mode d'interrogation automatisée visé par l'article 92. Elle a également évalué les conséquences de la duplication sur CD Rom de tout ou partie d'un N. SIS notamment à des fins d'interrogation par les représentations diplomatiques et consulaires.

L'examen des conditions d'application de l'article 102.2 a soulevé des questions relatives à la mise à jour des informations dupliquées et à la sécurité des transmissions effectuées vers des services situés en dehors des territoires des parties contractantes.

L'ACC a dès lors proposé une solution harmonisée compatible avec les règles de protection des données fixées par la Convention.

Dans son avis 97/1, elle a rappelé que, quels que soient les moyens retenus par les États membres pour organiser la consultation des signalements visés à l'article 96 de la Convention par leurs postes diplomatiques et consulaires, les principes de la Convention figurant ci-après devaient être respectés :
- les techniques et moyens de duplication doivent garantir l'identité de données en temps réel par rapport au traitement central SIS ;
- ces techniques et moyens de duplication doivent garantir les minima de protection à ceux exigés par l'article 118.1 de la Convention et plus particuliè rement des points b), d), f) de cet article ; ainsi que se conformer au prescrit de l'article 118.3 de la Convention ;
- le programme qui permet leur utilisation doit permettre un enregistrement répondant au prescrit de l'article 103 de la Convention.

Lesdits enregistrements doivent être rapatriés, tous les six mois et être tenus à la disposition de l'autorité de contrôle nationale visée à l'article 114 de la Convention auprès de l'instance qui a la compétence centrale pour la partie nationale du SIS visée à l'article 108.1 de la Convention.

En cas d'utilisation de moyens de duplication présentant un risque de manque d'identité de données, l'ACC recommande instamment que la partie contractante, qui engage de la sorte sa responsabilité, telle que prévue par les articles 92.2 et 116 de la Convention, s'oblige :
- en cas de signalement de l'individu dans le support de duplication utilisé, à faire une vérification en temps réel (réseau, téléphone, fax) afin de s'assurer de la confirmation de cette information ;
- en cas de non-signalement de l'individu dans le support de duplication utilisé, à accepter sa responsabilité en cas de signalement de ce même individu intervenue dans l'espace de temps entre la fixation des données sur le duplica teur et le temps réel. Cette responsabilité ne peut être supprimée que moyennant le preuve d'une vérification en temps réel au moment de la demande d'obtention du visa.

Lors de l'examen de cette question, l'ACC a constaté que, contrairement aux prescriptions de l'article 118.2, elle n'avait pas reçu communication des mesures particulières prises par chaque partie contractante pour assurer la sécurité des données lors de leur transmission à des services situés en dehors de leur territoire.

Elle a dès lors demandé au groupe central, le 6 décembre 1996, de lui préciser comment les États membres appliquaient l'article 118.2 de la Convention. Au moment de la rédaction du présent rapport, elle attend toujours ces informations, sur base desquelles elle vérifiera si les mesures appliquées respectent l'interprétation qu'elle a donné de la Convention.

Avis 98/1 du 3 février 1998 sur la conservation de dossiers après la suppression d'un signalement (SCH/Aut-cont (97) *55* rév. 2)

L'attention de l'ACC a été attirée sur les difficultés que soulève au regard de l'article 102.1 la conservation de dossiers relatifs à des signalements après suppression de ceux-ci.

L'article 102.1 interdit en effet aux parties contractantes d'utiliser les données prévues aux articles 95 à 100 pour d'autres fins que celles énoncées pour chacun des signalements visés à ces articles.

Or, les services de police nationaux de certaines parties contractantes conservent des dossiers relatifs à des signalement de l'article 95 et suivants de la Convention Schengen, même après leur suppression, et en font des dossiers pénaux.

Les autorités policières concernées s'appuient à cet effet sur les dispositions de leurs lois nationales (voir point 2.1.3. b) du manuel SIRENE), et sur les dispositions du titre VI de la Convention Schengen.

L'ACC a estimé qu'il s'agissait d'une question très importante au regard du principe de finalité des données. Dans son avis du 3 février 1998, elle a rappelé les principes et droits fondamentaux applicables en la matière, notamment les principes suivants :

a) Les données du SIS ne peuvent être fournies et utilisées qu'aux fins énoncées pour chacun des signalements concernés (articles 102 paragraphe 1 et 94 paragraphe 1). Toute dérogation à ce principe général doit être justifiée par la nécessité de la prévention d'une menace grave imminente pour l'ordre et la sécurité publics, pour des raisons graves de sûreté de l'État ou aux fins de la prévention d'un fait punissable grave (article 102 paragraphe 3).

b) Toute utilisation de données non conforme aux paragraphes 1 à 4 de l'article 102 est considérée comme détournement de finalité (article 102 para graphe 5).

c) Aux termes de l'article 112 de la Convention de Schengen, les données à caractère personnel intégrées dans le Système d'information Schen gen aux fins de la recherche de personnes ne sont conservées que pendant la durée nécessaire aux fins auxquelles elles ont été fournies.

d) Il résulte d'une interprétation complémentaire des dispositions conven tionnelles que ces principes s'appliquent à tout type de traitement de l'informa tion effectué en relation avec des signalements du Système d'information Schengen ou qui s'y réfère.

L'ACC a dès lors considéré que les mesures suivantes devaient être prises :

a) En cas de suppression d'un signalement aux fins de la recherche de personnes, chaque partie contractante Schengen, conformément à l'article 112 de la Convention, doit effacer celui-ci, et détruire sans délai tous les dossiers y relatifs.

b) Les instances Schengen doivent procéder à une révision du manuel SIRENE afin de supprimer les dispositions de son point 2.1.3 b), qui sont contraires à celles de la Convention de Schengen.

Avis 98/2 du 3 février 1998 sur l'usurpation d'identité et ses conséquences au regard du SIS pour le titulaire légitime de l'identité usurpée (SCH/Aut-cont (97) 42 rév. 2)

En cas d'usurpation d'identité, dans certains pays, l'auteur de l'usurpation d'identité est également signalé dans le SIS sous le nom de la personne dont l'identité a été usurpée.

En d'autres termes, le système contient un signalement avec une identité qui ne correspond ni de *facto* ni de jure à l'identité réelle de la personne recherchée. La personne dont l'identité a été usurpée se retrouve ainsi signalée dans le SIS sans en avoir été informée au préalable.

Certains États ont fait valoir qu'il fallait dans ce cas procéder immédiatement à la suppression des données relatives à la personne dont l'identité a été usurpée. D'autres estimaient que le signalement usurpé devait être maintenu même si la personne dont l'identité est indûment inscrite dans le SIS demande la suppression de ces données. L'argument invoqué en faveur du maintien du signalement est qu'il est nécessaire de rechercher l'usurpateur.

L'ACC a examiné les problèmes posés par l'utilisation abusive d'alias de personnes signalées dans le SIS, à la lumière des principes de protection des données à caractère personnel prévus par la Convention de Schengen. Elle a réaffirmé les principes et les droits fondamentaux en matière de protection des données, notamment :

a) Les données ne peuvent être fournies et utilisées qu'aux fins énoncées pour chacun des signalements (articles 102 paragraphe 1 et 94 paragraphe 1) ; il peut être dérogé à ce principe à titre exceptionnel pour prévenir une menace grave ou un fait punissable grave (article 102 paragraphe 3).

b) Toute utilisation des données non conforme aux paragraphes 1 à 4 de l'article 102 sera considérée comme détournement de finalité (article 102 paragraphe 5).

c) Toute personne a le droit d'exiger la rectification ou l'effacement des données la concernant, entachées d'erreurs de droit ou de fait (article 110).

d) Toute personne a le droit de saisir la juridiction ou l'autorité compé tente en vertu de la législation nationale d'une action en rectification ou en effacement (article 111 paragraphe 1).

e) Toute personne a le droit de demander la vérification des données, en étroite coordination avec l'autorité de contrôle nationale (article 114 para graphe 2).

L'ACC, tenant compte de manière proportionnelle et équilibrée des droits de la personne dont l'identité a été usurpée, prévus par la Convention de Schengen, ainsi que de la nécessité de détecter l'usurpateur, a émis l'avis suivant :

1) L'enregistrement dans le SIS de données concernant une personne dont l'identité a été usurpée est régi par le droit national, sans préjudice des règles plus rigoureuses de la Convention (article 104 paragraphe 1).

2) Toute partie contractante à l'origine d'un signalement est tenue de garantir que les données ne sont enregistrées qu'aux fins énoncées et qu'elles restent à jour et exactes (article 102 paragraphe 1, article 106 paragraphe 1, article 110, ainsi que les dispositions en matière de protection des données de

la Convention 108 du Conseil de l'Europe, notamment celles de l'article 5, qui lient les États Schengen).

3) Toute partie contractante à l'origine d'un signalement est tenue de garantir l'exercice du droit de rectification ou d'effacement des données enre gistrées, conformément à la procédure prévue à l'article 106.

4) Le maintien dans le SIS du signalement de personnes dont l'identité a été usurpée doit être évalué selon le principe de la proportionnalité, compte tenu d'une part des droits de la personne dont l'identité a été usurpée, et d'autre part de la nécessité de détecter l'usurpateur.

5) En attendant la mise en service du SIS II, il faut étudier et adopter une solution adéquate et, si possible, commune, permettant d'indiquer qu'il s'agit d'un signalement d'une identité usurpée. L'ACC exprime sa volonté de coopérer pour trouver une telle solution.

Avis 98/3 sur la transmission de données relatives aux véhicules volés depuis le SIS vers la banque de données d'Interpol « ASF [1] — Véhicules volés » (SCH/Aut-cont (97) 50 rév2)

Le projet en question, présenté dans une note du groupe OR. SIS, vise à transmettre vers une banque de données d'Interpol des données du SIS relatives aux personnes et aux véhicules volés et, ultérieurement, à d'autres catégories de données.

L'ACC a rappelé plusieurs principes de la Convention ainsi que son avis relatif au projet pilote Schengen sur les véhicules volés et, se référant uniquement aux aspects ayant trait à la protection des données à caractère personnel, a rendu l'avis suivant :

1) Les informations et données à caractère personnel enregistrées dans le Système d'information Schengen ne peuvent pas être transmises à Interpol dans le cadre du projet « ASF-véhicules volés » sans contrevenir aux dispositions de la Convention, en particulier aux articles 101, 102, 118 et 126.

2) Les données relatives à la marque, au type, à la couleur et aux caractéristiques techniques des véhicules, ne sont pas des données à caractère personnel au sens de la Convention.

3) La communication de données non personnelles à Interpol dans le cadre du projet « ASF-véhicules volés » n'enfreint pas les dispositions de la Convention en matière de protection des données pour autant qu'il n'y ait aucun lien possible vers une donnée permettant l'identification d'une personne en rapport avec ce véhicule.

1 *Automated Search Facility.*

4) L'échange d'informations dans le cadre de la coopération policière et au départ des fichiers nationaux est réglementé par la législation nationale concernée, et plus particulièrement la loi en matière de protection des données.

Avis 98/4 du 3 février 1998 sur l'interprétation de l'article 103 relatif au contrôle de l'admissibilité de l'interrogation du SIS (SCH/Aut-cont (97) 70 rév.)

L'attention de l'ACC a été attirée sur les difficultés apparues pour l'application de l'article 103 de la Convention relatif à l'enregistrement dans chaque N. SIS, par l'instance gestionnaire du fichier, de toute dixième transmission de données à caractère personnel en vue du contrôle de l'admissibilité de la consultation.

Consciente du fait que le Système d'information Schengen (SIS) est un système de recherche automatisé nécessitant une protection efficace contre l'accès non autorisé par des tiers, l'ACC a considéré que l'enregistrement d'une moyenne représentative des consultations du système est une méthode appropriée de lutte contre l'accès non autorisé par des tiers.

L'ACC a engagé une étude des solutions techniques adoptées par chaque État partie pour le respect de l'article 103.

Elle a constaté que les parties contractantes interprétaient de façon différente l'obligation que leur impose la Convention, d'enregistrer en moyenne toute dixième transmission de données à caractère personnel dans la partie nationale du Système d'information Schengen, en vue du contrôle de l'admissibilité de la consultation (article 103).

L'ACC a rendu un avis sur l'interprétation de cet article, afin d'harmoniser la procédure appliquée par les parties contractantes.

L'ACC estime que l'enregistrement prévu à l'article 103 doit répondre aux exigences minimales suivantes :

1) Une moyenne suffisamment représentative de toutes les consultations doit être enregistrée, qu'il y ait ou non une réponse positive. L'exigence minimale de 10 % d'enregistrements peut également être remplie par le biais d'enregis trements à intervalles réguliers.

2) Un enregistrement approprié comporte les éléments essentiels sui vants :

a) Les données biographiques transmises relatives à la personne qui fait l'objet de la consultation.

b) L'identification du terminal, ou de l'autorité qui a procédé à l'interro gation, en veillant à ce que toute mesure utile soit prise pour permettre l'identification de l'utilisateur.

c) Le lieu, la date et l'heure de la consultation.

d) Le motif de la consultation, par exemple l'indication de la base juridique du signalement.

3) En outre, il serait souhaitable d'indiquer les éléments suivants dans le cadre du contrôle de l'admissibilité de la consultation dans un cas concret : le numéro de dossier ou de main courante afin de retrouver le dossier ayant motivé la consultation, dans la mesure où il est disponible.

Les données sont exclusivement utilisées pour les finalités prévues à l'article 103.

Les données enregistrées doivent être effacées dans un délai de six mois.

L'ACC a insisté pour qu'il soit tenu compte de l'obligation découlant de l'article 103 conformément à son avis.

PROGRAMME D'ACTION

Le programme d'action proposé par le président de l'ACC pour le premier semestre 1998 a été approuvé le 3 février 1998.

Le programme vise l'approfondissement du rôle de l'ACC dans le cadre de Schengen, il définit les priorités de son intervention en faveur des principes de protection des données et recommande une coopération renforcée entre les instances Schengen.

L'ACC poursuivra sa mission de conseil et d'harmonisation des pratiques ou des doctrines nationales en rendant des avis. Elle s'assurera que les avis qu'elle a adoptés ont reçu de la part du groupe central la publicité nécessaire, faute de quoi, elle conviendra d'une méthode de publication des ceux-ci.

Une attention particulière sera consacrée au suivi par les organes exécutifs de Schengen des avis et recommandations de l'ACC, en particulier en ce qui concerne la sécurité du C.SIS.

En effet, si les deux présidences de Schengen qui se sont succédées durant l'année 1997 ont bien confié l'examen de ces recommandations à des groupes techniques, force est de constater que ce point n'a pas reçu la priorité qu'il doit revêtir selon l'ACC.

L'ACC souhaite que les instances Schengen lui fassent connaître très rapidement les suites qu'elles entendent réserver à ses recommandations. Il en est ainsi, notamment, de la demande de l'ACC de se voir attribuer un compte utilisateur, à des fins d'audit.

Cette solution lui permettrait d'accéder directement, sans pouvoir de modification, au système d'exploitation et aux bases de données, et de procéder ainsi plus facilement au contrôle du C.SIS.

En outre, la sécurité des bureaux SIRENE fera l'objet d'un contrôle spécifique dans tous les pays et, sur cette base, d'un rapport final.

L'ACC veillera à ce que le fascicule sur le droit d'accès et de communication des personnes aux informations les concernant enregistrées dans le SIS, dont elle a adopté le texte en décembre 1997, soit rendu disponible aux points de passage autorisés pour le franchissement des frontières extérieures de l'espace Schengen.

Elle renforcera ses contacts avec les représentants de l'Union européenne, dans la perspective de l'intégration de l'acquis Schengen dans l'Union européenne, notamment en participant à la définition de son acquis. Cette question revêtira une importance toute particulière dans le cadre du développement de systèmes européens de police.

Lors de la conférence de presse qu'elle organisera à Bruxelles le 28 avril 1998, elle présentera au public et à la presse son rapport annuel.

Le 30 juin 1998, elle organisera à Lisbonne un colloque sur le thème des droits des citoyens face aux systèmes d'information policiers, au travers du modèle Schengen.

Par la mise en œuvre de ce programme, l'ACC entend contribuer à renforcer son rôle ainsi que l'efficacité de son intervention en faveur des droits et des libertés des citoyens, dans le cadre de la consolidation de l'espace européen.

DECLARATION DES PAYS AYANT LE STATUT D'OBSERVATEURS

« Étant donné qu'ils disposent du statut d'observateurs au sein de l'ACC, les pays nordiques partagent les préoccupations exprimées dans le rapport annuel par les États Schengen qui sont membres à part entière. Ils partagent également les principaux points de vue qui y figurent. Ils considèrent entre autres qu'il est très important que les avis et opinions formulés soient observés et respectés par les instances centrales et nationales Schengen.

La présence des commissions nationales — en matière de protection des données et de la vie privée — des pays nordiques au sein de l'ACC revêt une importance considérable dans le cadre des efforts destinés à s'assurer que l'opinion publique accepte et soutienne la réalisation des activités importantes prévues par la Convention de Schengen. Les observateurs nordiques sont d'avis qu'il est possible que le budget de l'ACC doive être augmenté à l'avenir. Ils considèrent que les ressources administratives du secrétariat doivent être augmentées sans délai mais n'excluent pas le besoin de disposer d'une autorité plus formelle. »

Annexe 1
RAPPELS

Les instances communes pour l'application de la convention

Les parties contractantes ont, pour l'application de la Convention, créé deux instances :
- le Comité exécutif, composé d'un ministre responsable de la mise en œuvre de la Convention dans chaque État partie, est chargé de la mission générale de veiller à l'application correcte de la Convention et dispose par ailleurs de compétences particulières (article 131) ;
- l'autorité commune de contrôle (ACC), composée de deux représentants de chacune des Autorités nationales de contrôle des États parties a pour mission de vérifier la bonne exécution des dispositions de la Convention à l'égard de la fonction de support technique du SIS (article 115). Elle dispose également de compétences plus générales en matière de protection des données.

En dehors de ces deux instances, l'organisation de Schengen est structurée autour d'un groupe central dont dépend un comité d'orientation SIS ainsi que divers groupes de travail dont un seul est créé par la Convention [1]

Les instances Schengen sont assistées par un secrétariat, mis à leur disposition par le Bénélux, dont le siège est à Bruxelles.

Un organigramme figure en annexe.

L'objectif et l'architecture du SIS

L'intégralité du titre IV de la Convention est consacré au Système d'information Schengen (SIS).

L'article 93 de la Convention précise que le SIS a pour objet de préserver l'ordre et la sécurité publics, y compris la sûreté de l'État, et l'application des dispositions de la Convention sur la circulation des personnes à l'aide des informations transmises par le système.

LES INFORMATIONS ENREGISTREES

L'article 94 énumère limitativement les catégories de données qui peuvent être enregistrées dans le système. Les articles 95 à 100 spécifient les finalités qui justifient l'intégration des signalements.

[1] Il s'agit du « groupe permanent sur les stupéfiants », créé par l'article 70.

Les catégories de données se rapportent à des personnes, objets et véhicules.
— s'agissant des personnes, peuvent être intégrés les éléments relatifs à l'état civil et les alias, les signes physiques particuliers, objectifs et inaltérables, l'indication éventuelle qu'elles sont armées ou violentes et la conduite à tenir en cas de découverte.

Est interdite la mention d'informations dites sensibles révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que celles relatives à la santé ou à la vie sexuelle. Les finalités qui justifient le signalement d'une personne dans le SIS sont les suivantes :

a) Quelle que soit la nationalité de la personne :
- arrestation aux fins d'extradition (article 95) ;
- recherche en cas de disparition, recherche de mineurs ou de personnes devant être internées sur décision d'une autorité compétente (article 97) ;
- arrestation pour comparution, même en qualité de témoin, devant la justice dans le cadre d'une procédure pénale ou pour exécution d'une peine privative de liberté (article 98) ;
- surveillance discrète et contrôle spécifique pour la répression d'infractions pénales, la prévention de menaces pour la sécurité publique ou pour la prévention de menaces graves pour la sûreté de l'État (article 99).

b) Pour les étrangers, soit toute personne autre que des ressortissants des États membres des communautés européennes (définition dans l'article 1er, 6e alinéa).
- non admission sur le territoire résultant d'une décision administrative ou judiciaire prise dans le respect des règles de procédure nationales ou sur le fondement d'une menace à l'ordre public ou à la sécurité et sûreté nationales ou sur celui du non — respect des réglementations nationales sur l'entrée et le séjour des étrangers (article 96).
- s'agissant des objets, seuls peuvent être intégrés les éléments, incluant le nom de leur propriétaire, qui se rapportent aux véhicules, armes à feu documents et billets de banque volés, détournés ou égarés qui sont recherchés aux fins de saisie ou de preuve dans une procédure pénale (article 100).
- s'agissant des véhicules, peuvent également être enregistrées des données relatives à ceux qui sont recherchés aux fins de surveillance discrète ou de contrôle spécifique (article 99 déjà cité). Cette catégorie permet l'enregistrement d'informations concernant les conducteur et occupants des véhicules surveillés.

LES DESTINATAIRES DES INFORMATIONS

Les articles 92 et 101 de la convention précisent que les autorités désignées par les parties contractantes peuvent accéder, par une interrogation automatisée ou non :

- à l'ensemble des données enregistrées dans le SIS lors des contrôles de frontière et des vérifications et autres contrôles de police et de douane effectués à l'intérieur du pays conformément au droit national ;
- à la seule catégorie des signalements aux fins de non admission pour la délivrance des visas, des titres de séjour et l'administration des étrangers dans le cadre des dispositions de la convention concernant la circulation des personnes.

La liste des autorités qui peuvent interroger directement les données intégrées dans le SIS doit être communiquée au Comité exécutif (article 101.4).

L'ARCHITECTURE DU SYSTEME D'INFORMATION SCHENGEN

Si plusieurs des articles du titre IV prescrivent le respect de telle ou telle mesure d'ordre technique, la description générale du système figure dans l'article 92.

Le Système d'information Schengen (SIS) est composé d'une partie nationale (N. SIS) auprès de chacune des parties contractantes et d'une fonction de support technique (C.SIS) créée et entretenue en commun dont la responsabilité est assumée par la République française.

La fonction de support technique, installée à Strasbourg, a pour objet de rendre matériellement identiques tous les N. SIS. Pour cela le C.SIS comprend un fichier de données qui assure l'identité des fichiers nationaux par la transmission en ligne d'informations.

La transmission de données est effectuée conformément aux protocoles et procédures établis en commun par les parties contractantes pour la fonction de support technique.

L'article 118.4 précise les mesures de sécurité qui doivent être prises pour la fonction de support technique. Ces mesures sont identiques à celles requises pour chaque N. SIS (article 118.1 à 3).

Les bureaux SIRENE

Les bureaux SIRENE (Supplément d'informations requis à l'entrée nationale) sont une création des États-parties non expressément prévue par la Convention.

Chargés de procéder dans chaque État Schengen, sur la base du SIS, à des échanges d'informations complémentaires, ils servent également d'intermédiaires lors des diverses consultations d'État à État sur la conduite à tenir en cas d'exécution d'un signalement.

Leurs missions et actions sont définies de manière concrète dans un manuel commun dit « manuel SIRENE ». Pour l'essentiel, elles consistent en des consultations préalables à la création de signalements, des échanges d'informations et en la surveillance des signalements multiples et l'établissement d'ordres de priorité.

La protection des données à caractère personnel

UNE LOI ET UNE AUTORITÉ NATIONALE DE CONTRÔLE : CONDITIONS PRÉALABLES À L'APPLICATION DE LA CONVENTION

Les États parties ont posé plusieurs conditions préalables à l'application sur leur territoire de la Convention. Le caractère impératif de leur respect est rappelé dans l'acte final.

Au nombre de ces conditions figure l'obligation pour chaque État partie de se doter, avant toute transmission de données à caractère personnel, d'une autorité nationale de contrôle indépendante (articles 114 et 128) et d'une loi de protection des données.

Plus précisément, s'agissant du traitement automatisé ou non de données transmises en application de la Convention, la Convention comporte les prescriptions suivantes :

a) Pour le traitement automatisé de données transmises en application du titre IV relatif au SIS :

Article 117

Chaque partie contractante doit prendre au plus tard au moment de l'entrée en vigueur de la Convention les dispositions nationales nécessaires pour réaliser un niveau de protection des données à caractère personnel qui soit au moins égal à celui des principes découlant de 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, ce dans le respect de la recommandation R. (87) 15 du 17 septembre 1987 du comité des ministres du Conseil de l'Europe visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police.

La transmission de données à caractère personnel ne peut avoir lieu que lorsque les dispositions de protection des données à caractère personnel sont entrées en vigueur sur le territoire des parties contractantes concernées par la transmission.

b) Pour le traitement automatisé d'autres données transmises en appli cation de la Convention à l'exception de celles relatives aux demandes d'asile :

Article 126

Exigence, au moment de l'entrée en vigueur de la Convention, d'un niveau de protection des données à caractère personnel au moins égal à celui des principes découlant de la Convention du Conseil de l'Europe du 28 janvier 1981 sus-citée et transmission des données également subordonnée à l'effectivité de cette protection sur le territoire des parties contractantes concernées par la transmission.

Article 129

Pour la transmission des seules données relatives à la coopération policière, les parties contractantes doivent réaliser un niveau de protection des

données à caractère personnel qui, respecte les principes de la recommandation R. (87) 15 du 17 septembre 1987 du Comité des ministres du Conseil de l'Europe déjà mentionnée.

c) Pour les données transmises en application de la Convention prove nant d'un fichier ou intégrées dans un fichier à l'exception de celles qui se rapportent aux demandes d'asile, au SIS ou à l'entraide judiciaire en matière pénale

Article 127

Application des dispositions de l'article 126 et, pour la transmission de données relatives à la coopération policière, niveau de protection des données qui respecte les principes de la recommandation R. (87) sus-citée.

d) Enfin, s'agissant des données transmises qui figurent dans des dossiers, seules s'appliquent, à une exception près, les dispositions spécifiques de protection des données de l'article 126.3 sous le contrôle, le cas échéant, de l'autorité nationale compétente (article 128.2).

LES CHAMPS D'APPLICATION RESPECTIFS DE LA CONVENTION ET DU DROIT NATIONAL

La Convention opère, pour la protection des données à caractère personnel, une répartition complexe entre le champ d'application de ses dispositions et celui des droits nationaux des États-parties.

Les droits des personnes à l'égard du SIS

La règle peut s'énoncer ainsi : pour autant que la Convention ne prévoit pas de dispositions particulières, le droit de chaque partie contractante est applicable.

La Convention précise la nature des droits qui sont reconnus aux personnes et les limites éventuelles qui y sont apportées. Sous réserve du respect de ces dispositions, les droits des personnes s'exercent dans le respect du droit national de chaque État partie.

a) Droit d'accès et de communication (article 109).

Toute personne peut accéder aux informations la concernant intégrées dans le SIS. Pour cela elle peut former une demande auprès des instances compétentes de chacun des États-parties.

Si le droit national le prévoit, l'auteur de la demande peut se voir communiquer les informations qui le concernent. Toutefois en application du « principe de propriété des données », la communication est subordonnée au fait que l'État saisi qui n'est pas l'auteur de l'intégration donne préalablement à l'État signalant l'occasion de prendre position.

La communication des informations peut être refusée si elle peut nuire à l'exécution du signalement ou si elle s'avère nécessaire à la protection des droits et libertés d'autrui. Dans tous les cas, la communication est refusée si la personne est signalée aux fins de surveillance discrète.

b) Droit de rectification (article 110).

Toute personne peut, pour les données qui la concernent, faire rectifier celles qui sont entachées d'erreur de fait ou faire effacer celles qui sont entachées d'erreur de droit. Dans la pratique, l'exercice de ce droit est largement facilité par la communication des informations figurant dans le système.

c) Droit d'engager une action en rectification, en effacement, en information ou en indemnisation (article 111).

Toute personne doit pouvoir, sur le territoire de chaque partie contractante, faire valoir ses droits devant une juridiction ou toute autre autorité compétente. Les décisions définitives sont exécutées par l'État partie concerné.

d) Droit de demander une vérification des données (article 114.2).

Toute personne peut demander à une autorité nationale de contrôle de vérifier les données la concernant intégrées dans le SIS ainsi que l'utilisation qui en est faite. Si les données ont été intégrées par un autre État que celui auprès duquel la demande est introduite, le contrôle est effectué en étroite coordination avec l'autorité de contrôle de l'État signalant.

Le contrôle du Système d'information Schengen

La Convention énonce les principes de protection des données qui, sans préjudice du droit national de chaque partie contractante, sont applicables lors du traitement des données intégrées dans le SIS (article 104). Elle opère, pour le contrôle de leur respect, un partage entre l'ACC et les autorités nationale de contrôle (articles 114 et 115).

Les principes énumérés par la Convention sont les suivants.

a) Principe de finalité pour l'enregistrement des données et, sauf exceptions limitativement énumérées, pour leur utilisation : extradition, non-admission, personnes disparues, témoins, personnes citées ou condamnées, objets volés, personnes et véhicules sous surveillance discrète ou contrôle spécifique (articles 94 à 100 et 102 déjà cités).

b) Interdiction de traiter de données sensibles et énumération limitative des données enregistrées (article 94 déjà cité).

c) Définition des destinataires : accès limité aux autorités nationales compétentes dans certains domaines et pour le seul accomplissement de leurs missions (article 101 déjà cité).

d) Interdiction de copier les signalements d'une autre partie contractante dans un fichier national et limitation des duplications à des fins techniques (article 102).

e) Obligation d'enregistrement de toute dixième transmission de données aux fins de contrôle de l'admissibilité (article 103).

f) Fixation d'une durée de conservation des données (articles 112 et 113).

g) Obligation de conserver les données effacées durant une année dans la fonction de support technique aux fins de contrôle a *posteriori* de leur exactitude et de la licéité de leur intégration (article 113.2).

S'agissant du contrôle du système, la Convention précise que chaque État partie doit charger une autorité nationale de contrôler, de manière indépendante et dans le respect du droit national (article 114), le fichier de la partie nationale du système d'information (N. SIS). Il revient à ces autorités de vérifier le respect des dispositions de protection des données prévues par la Convention et celles qui s'y ajoutent le cas échéant en vertu du droit national.

En revanche, le contrôle de la fonction de support technique (C.SIS) est confié à l'ACC qui doit agir dans le respect de la Convention de Schengen, de la Convention du Conseil de l'Europe sur la protection des données, de la Recommandation du Conseil de l'Europe pour les données dans le secteur de la police et conformément au droit français.

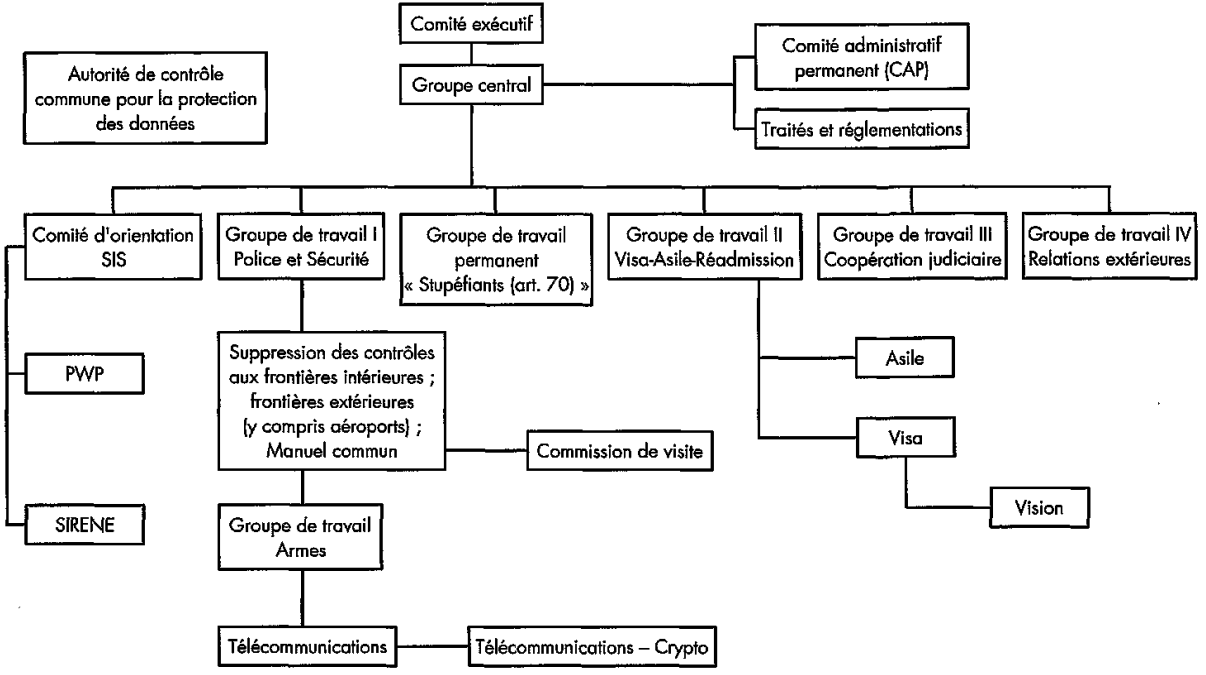
Les échanges d'informations hors le SIS

Le titre VI (articles 126 et suivants) de la Convention intitulé « protection des données à caractère personnel » est consacré aux règles applicables aux échanges d'informations qui ne donnent pas lieu à un enregistrement dans le SIS mais interviennent pour l'application de la Convention.

Les principes retenus (finalité, limitation des destinataires, exactitude des données...) sont applicables sans préjudice des dispositions du droit national de protection des données qui régit notamment l'exercice des droits des personnes concernées. Le contrôle du respect des règles énoncées par la Convention incombe aux autorités nationales.

L'ACC a un rôle résiduel : elle peut, à la demande des parties contractantes, émettre un avis sur les difficulté d'application et d'interprétation que soulèvent ces règles.

Annexe 2 – ORGANIGRAMME DES GROUPES DE TRAVAIL SCHENGEN



Annexe 3
AVIS RENDUS PAR L'AUTORITÉ DE CONTRÔLE COMMUNE

Avis du 7 mars 1997 sur le projet pilote relatif aux véhicules volés

L'ACC a été invitée à se prononcer sur un projet pilote relatif au trafic de véhicules volés. Il s'agit de savoir si les pays qui ne sont pas encore intégrés au Système d'information Schengen peuvent accéder aux données concernant les véhicules volés enregistrées dans le SIS. La demande d'avis ne contenait pas d'informations sur les aspects suivants du projet : les entités qui y participent, le système de coordination international et national, les conditions d'accès aux informations, et l'utilisation et l'analyse prévues de ces informations.

Dans l'intervalle, il a été possible d'obtenir les informations suivantes :

Le projet pilote a pour objectif d'améliorer la coordination policière européenne en matière de lutte contre le trafic de véhicules volés, et plus particulièrement en matière d'identification des réseaux internationaux de trafic, des itinéraires et des méthodes utilisées.

Les activités à accomplir, de manière coordonnée à différentes frontières et dans différentes régions définies au préalable, seront menées à bien par les forces de police qui, dans les différents États, sont chargées des contrôles frontaliers, routiers et douaniers ainsi qu'en matière fiscale et répressive.

Les États suivants participent au projet :

Les États parties à la Convention de Schengen qui ont introduit des signalements dans le SIS et ont accès à celui-ci (Allemagne, Belgique, Espagne, France, Luxembourg, Pays-Bas, Portugal).

Les États parties à la Convention de Schengen ou à des accords de coopération avec les États Schengen dans lesquels, pour différentes raisons, la Convention n'est pas encore appliquée, qui n'ont pas encore intégré des signalements dans le SIS ni n'accèdent au SIS (Autriche, Grèce, Italie, Danemark, Finlande, Norvège et Suède).

Se référant uniquement aux aspects ayant trait à la protection des données à caractère personnel,

L'ACC, considérant que

L'accès aux données intégrées dans le Système d'information Schengen ainsi que le droit de les consulter directement sont exclusivement réservés aux entités compétentes, énumérées dans une liste communiquée au Comité exécutif, qui définit la catégorie de signalement à laquelle chaque autorité a accès (le

droit d'accéder à une certaine catégorie de signalements et de les consulter, doit correspondre à la compétence nationale de chaque entité — article 101, paragraphes 1 et 3 de la Convention) ;

Les utilisateurs peuvent uniquement utiliser les données aux fins prévues pour chaque catégorie de signalement (finalité de l'utilisation — article 102 paragraphe 1) ;

Le droit national est applicable aux données intégrées dans la partie nationale du SIS, sauf conditions plus exigeantes prévues par la Convention (article 104, paragraphe 1) ;

La transmission de données à caractère personnel en application de la Convention peut uniquement s'effectuer vers les parties contractantes qui ont réalisé au niveau national un régime de protection des données à caractère personnel au moins égal à celui découlant des principes de la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 (article 126, paragraphes 1 et 2 de la Convention) ;

Les informations relatives à la marque, au type, à la couleur et aux caractéristiques techniques d'un véhicule ne constituent pas en soi des données à caractère personnel, s'il n'y a pas de lien entre ces informations et le numéro d'immatriculation, le propriétaire ou le conducteur du véhicule (ce qui permettra par exemple d'identifier un véhicule auprès du constructeur sans connaître le titulaire de l'immatriculation) ;

Au niveau de chaque pays participant au projet pilote, les autorités policières d'un autre État peuvent, via les mécanismes de la coopération policière, bilatérale ou multilatérale, accéder aux bases de données nationales des véhicules volés, dès lors que la législation nationale en matière de protection des données ne l'interdit pas ou l'autorise.

Informer les autorités compétentes de chaque pays participant sur le pays qui est à l'origine du signalement sans qu'une autre donnée ou un autre élément ne soit divulgué ne constitue pas une violation des dispositions de la Convention en matière de protection des données ;

Les échanges d'informations policières relatives aux véhicules volés au départ des fichiers nationaux, entre les parties contractantes intégrées au SIS et les autres États où la Convention n'est pas encore appliquée, relèvent des législations nationales en matière de protection des données et s'effectuent sous le contrôle des autorités de contrôle nationales.

Émet l'avis suivant

Les informations et données à caractère personnel enregistrées dans le Système d'information Schengen ne sont pas accessibles et ne peuvent pas être consultées directement par les autorités des parties contractantes où la Convention n'est pas encore mise en application, conformément aux articles 101 et 126, paragraphes 1 et 2 de la Convention.

Les données relatives à la marque, au type, à la couleur et aux caractéristiques techniques des véhicules ne sont pas, en soi, des données à caractère personnel aux fins de la Convention de Schengen.

La communication du pays signalant aux autorités compétentes des pays participant au projet n'enfreint pas les dispositions en matière de protection des données consignées dans la Convention, dès lors qu'aucune autre donnée n'est transmise.

L'échange d'informations dans le cadre de la coopération policière et au départ des fichiers nationaux est réglementé par la législation nationale concernée, et plus particulièrement la loi en matière de protection des données.

Avis du 7 mars 1997 sur l'accord de coopération concernant le traitement des infractions routières et l'exécution des sanctions pécuniaires y relatives

Le groupe central a sollicité l'avis de l'ACC sur l'accord de coopération relatif aux infractions routières SCH/III (96) 25, 4e rév.

L'accord consacre :

1) Le principe de la coopération entre les parties contractantes en matière de traitement des infractions routières et d'exécution des sanctions y relatives, en prévoyant la possibilité pour chaque service d'immatriculation national d'accéder, sur la base du numéro d'immatriculation, aux registres d'immatriculation des autres États pour obtenir des informations sur le véhicule (type et marque) ainsi que sur l'identité (nom et adresse) de la personne enregistrée comme propriétaire du véhicule au moment de la commission de l'infraction.

2) La communication directe des informations aux autorités compétentes des États qui demandent les informations, ainsi que du nom et de l'adresse de l'autorité requise.

3) L'information immédiate par l'autorité requérante des personnes suscep tibles d'avoir commis l'infraction, avec communication des informations permettant à la personne ou à l'entité en cause de réagir ou d'introduire un recours.

4) L'entraide des autorités en vue d'obtenir la réaction de l'intéressé.

5) Un système visant à limiter le montant des sanctions pécuniaires au montant prévu par la loi de l'État où elles sont exécutées.

6) La mission générale pour le Comité exécutif de Schengen de veiller à l'application de l'accord.

7) L'application des articles 126 à 128 de la Convention de Schengen à la transmission des données à caractère personnel.

L'ACC, qui s'est concentrée sur l'aspect relatif à la protection des données à caractère personnel, émet l'avis suivant :

a)L'accord relatif aux infractions routières est basé sur deux éléments essentiels : d'une part l'accès aux informations et aux données figurant dans les registres d'immatriculation des autres parties contractantes, dans les limites de leur finalité et des compétences des autorités nationales concernées, et d'autre part un système permettant la notification directe, la coopération ainsi que l'exécution effective par une partie contractante d'une décision émanant d'une autorité d'une autre partie contractante, à certaines conditions limitant l'appli cation d'une sanction pécuniaire, voire l'excluant (si la législation nationale ne prévoit pas l'infraction en question).

b) Les données ne peuvent être transmises qu'aux parties contractantes qui sont dotées d'une autorité de contrôle nationale indépendante et d'une loi sur la protection des données et qui garantissent un niveau de protection des données à caractère personnel au moins égal à celui découlant des principes de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (conformément aux articles 126 paragraphes 1 et 2 et 128 para graphe 1 de la Convention).

c) Les données à caractère personnel se limitent aux nom et adresse du propriétaire du véhicule et auteur présumé de l'infraction.

d) Les principes énoncés dans les articles 126 à 128 de la Convention s'appliquent à la transmission et à l'utilisation des données, ce qui implique que les données ne sont utilisées qu'aux fins pour lesquelles elles ont été transmises, à savoir l'identification et l'exécution d'une infraction routière en vue de l'exécution d'une sanction pécuniaire (principe de la finalité). De même, les données transmises ne peuvent être mises en relation avec des systèmes d'infor mation nationaux en matière d'infractions routières.

e) Le droit du titulaire des données d'être informé du fait que celles-ci ont été transmises est garanti, ainsi que le principe de la notification préalable à l'exécution de la sanction pécuniaire, et le droit de défense et de réaction, et partant la possibilité de s'opposer aux décisions fondées sur une erreur de fait ou de droit (articles 4 et 6 de l'accord).

L'ACC considère toutefois que les principes suivants devraient être intégrés ou explicités dans l'accord :

1) Le droit de toute personne d'exiger la rectification ou l'effacement de données la concernant qui sont entachées par une erreur de fait ou de droit.

2) Le principe de la coopération entre les autorités de contrôle nationales mentionnées à l'article 128 paragraphe 1 de la Convention en vue de garantir les droits d'accès, de rectification ou d'effacement.

3) La compétence de l'ACC d'émettre des avis sur les aspects communs en matière de protection des données à caractère personnel découlant de l'application de l'accord en question, ce principe devant être mentionné à l'article 16 du projet.

Avis n° 01/97 du 22 mai 1997 sur la duplication d'une partie des signalements du SIS

Objet : utilisation de supports techniques de duplication en vue de la consultation des signalements visés à l'article 96 de la Convention d'application des accords de Schengen par les postes diplomatiques et consulaires de certains États Schengen à l'étranger.

Lors de la réunion du 22 mai 1997, l'autorité de contrôle commune (ci-après ACC) a, sur base de l'article 115.3 et 126 f de la Convention d'application des accords de Schengen (ci-après CAS), adopté l'avis suivant au sujet du problème repris sous rubrique :

- constatant que les postes diplomatiques et consulaires de certaines parties Contractantes (ex. la Belgique, l'Espagne, les Pays-Bas et la France) utilisent divers moyens techniques afin de faciliter la consultation sur place des signale ments visés à l'article 96 CAS ;
- que ces consultations sont opérées en vue de la délivrance d'un visa d'entrée sur le territoire Schengen conformément aux articles 92.1 *in fine* CAS et 101.2 CAS;
- qu'un système d'interrogation directe du SIS n'est pas toujours disponible aux postes diplomatiques et consulaires de certaines parties contractantes et cela pour de multiples raisons.

L'ACC a procédé à la vérification de leur comptabilité avec le modèle initial du SIS tel que développé dans la CAS

En effet, plusieurs dispositions de la CAS imposent des conditions strictes quant aux procédures d'utilisation du SIS :

a) Plusieurs passages de l'article 92 CAS développent « une procédure d'interrogation directe » (art. 92.1 CAS) basée sur une « transmission rapide et efficace des données » (art. 92.2, CAS).

L'article 92.3 CAS, précise d'ailleurs que la fonction de support technique, appelée plus communément C-SIS, comprend un fichier de données assurant l'identité des fichiers de données des différents N-SIS « par la transmission en ligne d'informations ».

En outre, l'article 101.2 CAS, habilitant différentes autorités à accéder aux signalements visés à l'article 96 CAS, évoque également le mode « d'interrogation directe » précisément dans le chef d'instances chargées de la délivrance des visas et d'instances centrales compétentes pour l'examen des demandes de visa.

Enfin, le processus d'interrogation directe est à nouveau mentionné à l'article 101.4 CAS, ainsi qu'à l'article 102.2 CAS et l'article 106.2 CAS évoque, quant à lui, l'éventualité de corrections ou d'effacements c'est-à-dire de modifications ou de mises à jour des données « sans délai » et imposées à charge de chaque partie contractante.

Il ressort de ces différents passages du titre IV de la CAS que le mode de traitement de l'information, que les auteurs de la CAS ont voulu développer, fait référence à un système d'interrogation automatisée de données permettant des traitements de données en temps réel.

b) La CAS prévoit un certain nombre de dispositions de sécurité.

L'article 118.1 CAS exige de chaque partie contractante un ensemble de garanties visant à protéger les données à caractère personnel intégrées dans le SIS.

Parmi celles-ci, l'ACC relève notamment :
- les mesures propres « à empêcher que des supports de données ne puissent être lus, copiés, modifiés ou éloignés par une personne non autorisée (contrôle des supports de données) » (art. 118.1. b) CAS) ;
- les mesures propres « à garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission) » (art. 118.1. f) CAS);
- les mesures propres « à empêcher que, lors de la transmission des données à caractère personnel ainsi que lors du transport des supports de données, les données ne puissent être lues, modifiées ou effacées de façon non autorisée (contrôle de transport) » (article 118.1. b). CAS).

c) En outre, des exigences d'enregistrement en vue de contrôle sont prévues.

L'article 103. CAS recommande à chaque partie contractante d'enregistrer toute dixième transmission de données à caractère personnel aux fins de contrôle de l'admissibilité de l'interrogation.

Suite à une question de l'autorité de contrôle commune provisoire, en janvier 1994 (voir note SCH/Aut-cont (94) 33 du 10 janvier 1994), le représentant du Comité d'orientation a précisé que l'interprétation qui est donnée à cet article va dans le sens d'un enregistrement minimal de toute dixième réponse positive (cf. note SCH/OR. SIS (95) 116 du 16 juin 1995).

Par ce motif, l'ACC

Est d'avis que l'utilisation de moyens de duplication, quelque soit leur forme (CD Rom, disquette...) en vue de la consultation des signalements visés à l'article 96 de la CAS par les postes diplomatiques et consulaires de certains États Schengen à l'étranger est soumise à trois conditions essentielles :

1) Les techniques et moyens de duplication doivent garantir l'identité de données en temps réel par rapport au traitement central SIS Tout décalage dans le temps, aussi minime soit il, doit se conformer aux conditions prévues sous 4.

2) Ils doivent garantir les minima de protection à ceux exigés par l'article 118.1 CAS et plus particulièrement des points b), d), f) de cet article ; ainsi que se conformer au prescrit de l'article 118.3 CAS.

3)Le programme qui permet leur utilisation doit permettre un enregistre ment répondant au prescrit de l'article 103 CAS ;

Lesdits enregistrements doivent être rapatriés, tous les six mois et être tenus à la disposition de l'autorité de contrôle nationale visée à l'article 114 CAS auprès de l'instance qui a la compétence centrale pour la partie nationale du SIS visée à l'article 108.1 CAS.

4) En cas d'utilisation de moyens de duplication présentant un risque de manque d'identité de données, l'ACC recommande instamment que la partie contractante, qui engage de la sorte sa responsabilité, telle que prévue par les articles 92.2 et 116 de la CAS, s'oblige :
- en cas de signalement de l'individu dans le support de duplication utilisé, de faire une vérification en temps réel (réseau, téléphone, fax) afin de s'assurer de la confirmation de cette information ;
- en cas de non-signalement de l'individu dans le support de duplication utilisé, à accepter sa responsabilité en cas de signalement de ce même individu intervenue
dans l'espace de temps entre la fixation des données sur le duplicateur et le temps réel. Cette responsabilité ne peut être supprimée que moyennant le preuve d'une vérification en temps réel au moment de la demande d'obtention du visa.

Avis n° 98/1 du 3 février 1998 sur la conservation de dossiers après la suppression d'un signalement

Lors de sa réunion du 3 février 1998, l'autorité de contrôle commune (ci-après « ACC ») a, sur la base de l'article 115 paragraphe 3 de la Convention de Schengen, adopté l'avis suivant :

Consciente du fait que les services de police nationaux de certaines parties contractantes conservent des dossiers relatifs à des signalements de l'article 95 et suivants de la Convention de Schengen même après la suppression de ces signalement et qu'ils en font des dossiers pénaux, et que les autorités policières concernées s'appuient à cet effet sur les dispositions de leur loi nationale sur la protection des données (voir point 2.1.3 b) du manuel SIRENE), les dispositions du titre VI de la Convention de Schengen s'appliquant également, l'autorité de contrôle commune a procédé à un examen de cette pratique et, dans ce contexte, met tout particulièrement en évidence les exigences suivantes en matière de protection des données.

L'autorité de contrôle commune confirme les principes et droits fondamentaux en matière de protection des données prévus par la Convention de Schengen, notamment les principes suivants :

a) Les données ne peuvent être fournies et utilisées qu'aux fins énoncées pour chacun des signalements concernés (articles 102 paragraphe 1 et 94 paragraphe 1). Toute dérogation à ce principe général doit être justifiée par la nécessité de la prévention d'une menace grave imminente pour l'ordre et la

sécurité publics, pour des raisons graves de sûreté de l'État ou aux fins de la prévention d'un fait punissable grave (article 102 paragraphe 3).

b) Toute utilisation de données non conforme aux paragraphes 1 à 4 de l'article 102 sera considérée comme détournement de finalité (article 102 paragraphe 5).

c) Aux termes de l'article 112 de la Convention de Schengen, les données à caractère personnel intégrées dans le Système d'information Schen gen aux fins de la recherche de personnes ne sont conservées que pendant la durée nécessaire aux fins auxquelles elles ont été fournies.

d) Il résulte d'une interprétation complémentaire des dispositions conven tionnelles que ces principes s'appliquent à tout type de traitement de l'informa tion effectué en relation avec des signalements du Système d'information Schengen ou qui s'y réfère.

L'autorité de contrôle commune considère dès lors que les mesures suivantes doivent être prises :

a) En cas de suppression d'un signalement aux fins de la recherche de personnes, chaque partie contractante Schengen, conformément à l'article 112 de la Convention, doit effacer celui-ci, et détruire sans délai tous les dossiers y relatifs.

b) Les instances Schengen doivent procéder à une révision du manuel SIRENE afin de supprimer les dispositions de son point 2.1.3 b), qui sont contraires à celles de la Convention de Schengen.

Avis n° 98/2 du 3 février 1998 sur le signalement dans le SIS de personnes dont l'identité à été usurpée

L'ACC a examiné les problèmes posés par l'utilisation abusive d'alias de personnes signalées dans le SIS (cf. notes SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 et SCH/Aut-cont (97) 42), à la lumière des principes de protection des données à caractère personnel prévus par la Convention de Schengen.

Le signalement du titulaire légitime dont l'identité a été usurpée est maintenu dans le SIS dans la majorité des États. Actuellement, il ne semble pas possible de préciser dans le SIS, du moins en texte libre, qu'il s'agit d'une usurpation d'identité.

L'ACC réaffirme les principes et les droits fondamentaux en matière de protection des données, notamment :

a) Les données ne peuvent être fournies et utilisées qu'aux fins énoncées pour chacun des signalements (articles 102 paragraphe 1 et 94 paragraphe 1) ; il peut être dérogé à ce principe à titre exceptionnel pour prévenir une menace grave ou un fait punissable grave (article 102 paragraphe 3).

b) Toute utilisation des données non conforme aux paragraphes 1 à 4 de l'article 102 sera considérée comme détournement de finalité (article 102 paragraphe 5).

c) Toute personne a le droit d'exiger la rectification ou l'effacement des données la concernant, entachées d'erreurs de droit ou de fait (article 110).

d) Toute personne a le droit de saisir la juridiction ou l'autorité compé tente en vertu de la législation nationale d'une action en rectification ou en effacement (article 111 paragraphe 1).

e) Toute personne a le droit de demander la vérification des données, en étroite coordination avec l'autorité de contrôle nationale (article 114 paragraphe 2).

L'ACC, tenant compte de manière proportionnelle et équilibrée des droits de la personne dont l'identité a été usurpée, prévus par la Convention de Schengen, ainsi que de la nécessité de détecter l'usurpateur, émet l'avis suivant :

1) L'enregistrement dans le SIS de données concernant une personne dont l'identité a été usurpée est régi par le droit national, sans préjudice des règles plus rigoureuses de la Convention (article 104 paragraphe 1).

2) Toute partie contractante à l'origine d'un signalement est tenue de garantir que les données ne sont enregistrées qu'aux fins énoncées et qu'elles restent à jour et exactes (article 102 paragraphe 1, article 106 paragraphe 1, article 110, ainsi que les dispositions en matière de protection des données de la Convention 108 du Conseil de l'Europe, notamment celles de l'article 5, qui lient les États Schengen).

3) Toute partie contractante à l'origine d'un signalement est tenue de garantir l'exercice du droit de rectification ou d'effacement des données enre gistrées, conformément à la procédure prévue à l'article 106.

4) Le maintien dans le SIS du signalement de personnes dont l'identité a été usurpée doit être évalué selon le principe de la proportionnalité, compte tenu d'une part des droits de la personne dont l'identité a été usurpée, et d'autre part de la nécessité de détecter l'usurpateur.

5) En attendant la mise en service du SIS II, il faut étudier et adopter une solution adéquate et, si possible, commune, permettant d'indiquer qu'il s'agit d'un signalement d'une identité usurpée. L'ACC exprime sa volonté de coopérer pour trouver une telle solution.

Avis n° 98/3 du 3 février 1998 sur les relations éventuelles entre le SIS et le système en projet « ASF-vehicules volés » d'Interpol

L'ACC a été saisie d'une note de la délégation allemande du groupe OR. SIS (document SCH/OR. SIS (97) 81) du 30 avril 1997 qui présente le projet ASF-véhicules volés *(Automated Search Facility)* en vue d'une prise de

position dans le cadre de Schengen à l'égard d'Interpol. Le projet amène l'ACC à se poser la question de savoir si les données du SIS relatives aux personnes et aux véhicules volés peuvent être transmises à Interpol.

La note précitée donne une description succincte du projet : « D'après les informations dont dispose la délégation allemande, seuls quatre États (Suède, Luxembourg, Russie et Slovaquie) participent pour l'heure actuelle au projet relatif aux véhicules volés, dans le contexte duquel des données relatives à quelques 80 000 véhicules volés sont disponibles [...]. Il s'agit à cet égard des données relatives aux personnes et aux véhicules volés [...] ».

Une extension de ce projet à d'autres catégories de données est également envisagée dans la note précitée (œuvres d'art volées, cartes de crédit, documents et passeports falsifiés, bateaux/avions volés). Vu l'importance que de tels projets peuvent prendre à l'avenir, l'ACC a décidé d'émettre un avis sur ce projet en apportant une réponse à la question de savoir si les données du SIS relatives aux personnes et véhicules volés peuvent être transmises à Interpol dans le cadre du projet ASF.

Se référant uniquement aux aspects ayant trait à la protection des données à caractère personnel,

L'ACC, considérant que :

a) En vertu de l'article 101 4 de la Convention, seules les autorités compétentes sont autorisées à interroger directement les données intégrées dans le SIS. A cet égard, chaque partie contractante communique au Comité exécutif la liste des ces autorités, en indiquant pour chacune d'elles, les données qu'elles peuvent interroger, et pour quelles missions.

b) En vertu de l'article 102 1 de la Convention, les données ne peuvent être utilisées par les parties contractantes qu'aux fins prévues pour chaque catégorie de signalement.

En vertu de l'article 102 2 de la Convention, la duplication des données est interdite (sauf à des fins techniques, nécessaire pour l'interrogation directe par les autorités compétentes) ;

En vertu de l'article 102 4 de la Convention, les données ne peuvent pas être utilisées à des fins administratives ;

Enfin, en vertu de l'article 102 5 de la Convention, toute utilisation non conforme aux paragraphes précités de ce même article est considérée comme un détournement de finalité ;

c) En vertu de l'article 104 1 de la Convention, le droit national est applicable aux données intégrées dans la partie nationale du SIS, sauf condi tions plus exigeantes prévues par la Convention.

d) En vertu de l'article 126, 1 et 2 de la Convention, les transmissions de données à caractère personnel prévues par la Convention ne peuvent s'opérer que vers les parties contractantes qui ont pris les dispositions nationales

nécessaires aux fins de réaliser un niveau de protection de ces données qui soit au moins égal à celui découlant des principes de la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981.

e) En vertu de l'article 118, point d, chaque partie contractante s'engage à prendre, pour la partie nationale du SIS, les mesures propres à empêcher que des systèmes de traitement automatisés de données ne puissent être utilisés par des personnes non autorisées à l'aide d'installation de transmission de données ;

f) Les données relatives à la marque, au type, à la couleur et aux caractéristiques techniques des véhicules, ne sont pas des données à caractère personnel, pour autant qu'il n'y ait pas de lien possible vers une donnée permettant l'identification d'une personne en rapport avec ce véhicule, comme par exemple, le numéro d'immatriculation ou le numéro de châssis, pouvant conduire à l'identification du propriétaire du véhicule ou de son conducteur.

g) Les autorités policières de chaque pays participant au projet ASF, peuvent échanger des informations (en l'occurrence de données à caractère personnel) provenant de bases de données nationales, dans la mesure où, par le biais de mécanismes de coopération policière, bilatérale ou multilatérale, cet échange est autorisé ou n'est pas interdit par la législation nationale en matière de protection de données.

h) 11 doit être tenu compte de l'avis du 7 mars 1997 que l'ACC a rendu à l'égard d'un projet pilote relatif aux véhicules volés (voir Document SCH/Aut-cont (97) 22 rev.). Dans cet avis, il s'agissait de déterminer si les pays qui ne sont pas encore intégrés au Système d'information Schengen peuvent accéder aux données concernant les véhicules volés enregistrés dans le SIS.

Émet l'avis suivant :

1) Les informations et données à caractère personnel enregistrées dans le Système d'information Schengen ne peuvent pas être transmises à Interpol dans le cadre du projet « ASF-véhicules volés » sans contrevenir aux dispositions de la Convention, en particulier aux articles 101, 102, 118 et 126.

2) Les données relatives à la marque, au type, à la couleur et aux caractéristiques techniques des véhicules, ne sont pas des données à caractère personnel au sens de la Convention.

3) La communication de données non personnelles à Interpol dans le cadre du projet « ASF-véhicules volés » n'enfreint pas les dispositions de la Convention en matière de protection des données pour autant qu'il n'y ait aucun lien possible vers une donnée permettant l'identification d'une personne en rapport avec ce véhicule.

4 L'échange d'informations dans le cadre de la coopération policière et au départ des fichiers nationaux est réglementé par la législation nationale concernée, et plus particulièrement la loi en matière de protection des données.

Avis n° 98/4 du 3 février 1998 sur l'enregistrement des consultations prévu a l'article 103 de la convention

L'autorité de contrôle commune,

Vu l'article 115 de la Convention d'application de l'accord de Schengen ;

Consciente du fait que le Système d'information Schengen (SIS) est un système de recherche automatisé nécessitant une protection efficace contre l'accès non autorisé par des tiers ;

Que l'enregistrement d'une moyenne représentative des consultations du Système est une méthode appropriée de lutte contre l'accès non autorisé ;

Que l'article 103 de la Convention d'application impose à chaque partie contractante de veiller à ce l'instance gestionnaire du fichier enregistre en moyenne toute dixième transmission de données à caractère personnel dans la partie nationale du Système d'information Schengen, en vue du contrôle de l'admissibilité de la consultation ;

Considère que l'enregistrement prévu à l'article 103 doit répondre aux exigences minimales suivantes :

1) Une moyenne suffisamment représentative de toutes les consultations doit être enregistrée, qu'il y ait ou non une réponse positive. L'exigence minimale de 10 % d'enregistrements peut également être remplie par le biais d'enregis trements à intervalles réguliers.

2) Un enregistrement approprié comporte les éléments essentiels suivants :

a) Les données biographiques transmises relatives à la personne qui fait l'objet de la consultation.

b) L'identification du terminal, ou de l'autorité qui a procédé à l'interro gation, en veillant à ce que toute mesure utile soit prise pour permettre l'identification de l'utilisateur.

c) Le lieu, la date et l'heure de la consultation.

d) Le motif de la consultation, par exemple l'indication de la base juridique du signalement.

3) En outre, il serait souhaitable d'indiquer les éléments suivants dans le cadre du contrôle de l'admissibilité de la consultation dans un cas concret :

Le numéro de dossier ou de main courante afin de retrouver le dossier ayant motivé la consultation, dans la mesure où il est disponible.

4) Les données sont exclusivement utilisées pour les finalités prévues à l'article 103.

5) Les données enregistrées doivent être effacées dans un délai de six mois.

L'ACC insiste pour qu'il soit tenu compte de l'obligation découlant de l'article 103 conformément au présent avis.

Annexe 4
RÈGLEMENT INTÉRIEUR DE L'AUTORITÉ DE CONTRÔLE COMMUNE

Approuvé par l'ACC le 2 février 1996, modifié en son article 2 par décision prise par l'ACC lors de sa réunion du 04 juillet 1997

L'autorité de contrôle commune,

Vu l'article 115 de la Convention d'application de l'accord de Schengen du 14 juin 1985, relatif à la suppression graduelle des contrôles aux frontières communes, signée le 19 juin 1990, ci-après « la Convention »

Adopte, le 19 octobre 1995, le règlement intérieur suivant :

ARTICLE 1er — COMPÉTENCE

1) l'autorité de contrôle commune remplit, conformément au présent règlement intérieur, les missions qui lui sont dévolues par la Convention, ainsi que d'autres missions relatives à la protection des données à caractère personnel dont elle estime qu'elles sont liées à l'application de la Convention.

2) Dans l'exercice de ses missions, l'autorité de contrôle commune peut intervenir, soit d'office, soit à la demande d'une autorité de contrôle nationale d'un État Schengen, d'une partie contractante ou d'une instance du Système Schengen, conformément aux dispositions de la Convention.

ARTICLE 2 — COMPOSITION

1) Conformément aux dispositions de l'article 115, l'autorité de contrôle commune comprend deux représentants de l'autorité nationale, visée à l'article 114, de chaque partie contractante pour laquelle la Convention est entrée en vigueur conformément à l'article 140. Par partie contractante on entend aussi les parties ayant conclu avec les parties à l'accord et à la Convention de Schengen un accord de coopération concernant la suppression des contrôles de personnes aux frontières intérieures telles que définies à l'article 1er de la Convention dans la mesure où l'accord de coopération est mis en vigueur. Chaque délégation dispose d'une voix délibérative.

2) l'autorité de contrôle commune peut, par une décision prise à l'unanimité, accorder le statut d'observateur sans voix délibérative aux représentants des autorités nationales de contrôle visées à l'article 114, ou aux experts indépendants d'une partie contractante qui ne remplit pas encore les conditions de l'article 140, 2) dernière phrase. Par partie contractante on entend également une partie ayant conclu avec les États parties à l'accord et à la Convention de Schengen un accord de coopération sur la suppression des

contrôles aux frontières intérieures telles que définies à l'article 1er de la Convention si cet accord a été ratifié, approuvé ou accepté par toutes les parties contractantes, mais n'est pas encore entré en vigueur.

3) Les membres de l'autorité de contrôle commune ainsi que les obser vateurs ne peuvent pas être membres d'un groupe de travail ou d'une autorité — autre que l'autorité nationale de contrôle sur la protection des données à caractère personnel — institués en vertu de la Convention. Ils peuvent toutefois se joindre en tant qu'experts à leurs délégations nationales.

4) Un membre de l'autorité de contrôle commune empêché d'assister à une réunion peut être remplacé par une personne désignée par l'autorité de contrôle nationale conformément au présent article.

5) Les membres de l'autorité de contrôle commune peuvent se faire accompagner d'un expert qui les assiste.

ARTICLE 3 — PRESIDENCE

1) L'autorité de contrôle commune élit, parmi ses membres, son président et son vice-président. Ceux-ci sont élus à la majorité de deux tiers des délégations visées à l'article 2, paragraphe 1. Leur mandat a une durée d'un an, renouvelable une fois.

2) Le vice-président fait partie d'une autre délégation que le président ; il remplace le président en cas d'absence ou d'empêchement.

3) Si une vacance se produit avant l'expiration du mandat du président ou du vice-président, il est pourvu à son remplacement. Le membre élu en remplacement assure ses fonctions pour la durée du mandat restant à courir.

ARTICLE 4 — ROLE DU PRESIDENT

1) Le président représente l'autorité de contrôle commune. Il veille à son bon fonctionnement. Il convoque l'autorité et fixe le lieu, le jour et l'heure des réunions. Il ouvre et lève les séances. Il dirige les débats. Le président établit l'ordre du jour provisoire.

2) En vue de préparer les délibérations de l'autorité de contrôle commune, le président peut désigner, pour un sujet déterminé, un ou plusieurs rapporteurs parmi les membres.

ARTICLE 5 — FONCTIONNEMENT

1) L'autorité de contrôle commune se réunit au moins deux fois par an. Elle se réunit également sur l'initiative du président ainsi que chaque fois qu'au moins trois délégations visées à l'article 2, paragraphe 1, formulent une

demande motivée en ce sens, oralement au cours d'une réunion ou par écrit. Enfin elle se réunit dans les cas prévus par la Convention.

2) Sauf dans les cas jugés urgents par le président, les convocations sont transmises au moins quatorze jours avant la date de la réunion. La convocation comporte l'ordre du jour provisoire ainsi que, dans la mesure du possible, les documents nécessaires aux débats.

3) L'autorité de contrôle commune adopte l'ordre du jour définitif au début de chaque réunion.

ARTICLE 6 — QUORUM ET RÈGLES DE MAJORITÉ

1) L'autorité de contrôle commune ne peut se réunir valablement que lorsque les deux tiers au moins de délégations visées à l'article 2, paragraphe 1, sont présentes.

2) Sous réserve des dispositions de l'article 13, les actes de l'autorité de contrôle commune sont adoptés lorsque la moitié plus une des délégations présentes visées à l'article 2, paragraphe 1, s'expriment favorablement.

3) Chaque délégation peut déposer une note d'explication de vote.

4) L'autorité de contrôle commune délibère sur la base de documents et de projets rédigés dans les langues nationales de tous les États Schengen.

ARTICLE 7 — PUBLICITE ET DESTINATAIRES DES ACTES

1) Sauf décision contraire de l'autorité de contrôle commune, les réunions de celle-ci ne sont pas publiques.

2} L'autorité de contrôle commune détermine les destinataires de ses actes et se prononce sur la publicité éventuelle de ceux-ci, sans préjudice des dispositions de l'article 115, paragraphe 4 de la Convention.

ARTICLE 8 — PROCEDURE ECRITE

1) Les actes de l'autorité de contrôle commune peuvent être adoptés par le biais d'une procédure écrite, à condition que toutes les délégations en aient accepté le principe au cours d'une réunion.

2) En cas d'urgence, le président peut recourir d'office à la procédure écrite.

3) Dans les deux cas, le président transmet un projet à tous les membres de l'autorité de contrôle commune. Les délégations qui n'ont pas fait valoir d'observations dans un délai, à fixer par le président, d'au moins quatorze jours à compter de la date de réception du projet, sont réputés avoir approuvé le projet.

4) Il est mis fin à la procédure écrite dans le cas prévu au paragraphe 2 du présent article si une délégation demande, dans un délai de cinq jours ouvrables à compter de la date de réception du projet, que ce dernier fasse l'objet d'une discussion au sein de l'autorité de contrôle commune.

ARTICLE 9 — GROUPES DE TRAVAIL, EXPERTS, VÉRIFICATIONS SUR PLACE

1) L'autorité de contrôle commune peut instituer des groupes de travail dont elle définit la mission.

2) L'autorité de contrôle commune peut faire appel à des experts. Elle peut dresser une liste d'experts auxquels il est fait appel en priorité.

3) S'agissant du contrôle de la fonction de support technique, l'autorité de contrôle commune peut désigner un ou plusieurs de ses membres pour procéder à des vérifications sur place. S'il le juge urgent, le président peut procéder d'office à une telle désignation. Dans ce cas, il en informe sans délai les membres de l'autorité de contrôle commune. Les membres chargés d'effectuer des vérifications peuvent se faire assister par des experts inscrits sur la liste précitée.

4) Les groupes de travail, les experts et les membres de l'autorité chargés de procéder à des vérifications rendent compte des résultats de leurs missions à l'autorité de contrôle commune.

ARTICLE 10 — SECRETARIAT

1) Le secrétariat de l'autorité de contrôle commune est assuré sous la responsabilité du président par les personnes et les services mis à disposition par l'autorité compétente de la coopération Schengen.

2) Le secrétariat tient un registre des actes adoptés par l'autorité de contrôle commune.

3) Le courrier destiné à l'autorité de contrôle commune est adressé au secrétariat, à l'attention du président.

ARTICLE 11 — PROCES-VERBAUX

1) Un procès-verbal est dressé pour chaque réunion de l'autorité de contrôle commune.

2) Le projet de procès-verbal est rédigé par le secrétariat, sous la responsabilité du président. Il est soumis à l'approbation de l'autorité de contrôle commune lors de la réunion suivante.

3) Les membres et les observateurs peuvent faire rectifier le procès-verbal ultérieurement en fonction des remarques qu'ils ont formulées lors de la réunion concernée.

ARTICLE 12 — CONFIDENTIALITE

Sans préjudice de l'application de l'article 7, paragraphe 2, les membres de l'autorité de contrôle commune, les observateurs, les experts et les membres du secrétariat sont tenus de respecter la confidentialité. Cette obligation ne s'applique ni à l'égard des autorités de contrôle nationales ni à l'égard des autres autorités nationales auxquelles les membres et les observateurs doivent faire rapport conformément au droit national.

ARTICLE 13 — MODIFICATION DU RÈGLEMENT

L'autorité de contrôle commune adopte, à l'unanimité, les dispositions visant à modifier le présent règlement. Sauf disposition contraire, ces dispositions entrent en vigueur une semaine après leur adoption.

Annexe 5
LISTE DES MEMBRES DE L'AUTORITÉ DE CONTRÔLE COMMUNE

Belgique

M. Thomas (jusqu'au 19 janvier 98), Commission de la protection de la vie privée
Bld de Waterloo 115 -1000 Bruxelles

M. B. De Schutter, Commissie voor de bescherming van de persoonlijke levenssfeer
Vrije Universiteit Brussel, Pleinlaan 2 -1050 Brussel
Tél: 00 32 2 629 21 11
Fax : 00 32 2 629 36 33

M^{me} B. Havelange, Commission de la protection de la vie privée
Bld de Waterloo 115 -1000 Bruxelles
Tél : 00 32 2 542 72 00
Fax : 00 32 2 542 72 12

Pays-Bas

MM. P.J. Hustinx & P.A. Michael, Registratiekamer
Prins Clauslaan 20, Postbus 93374
25090AJ 's-Gravenhage
Tél :00 31 70 381 13 00
Fax: 00 31 70 381 13 01

Espagne

M. D. Juan Maria Bandres Molet
San martin 13 4°
20005 San Sébastian
Tél : 00 34 43 42 24 70
Fax: 00 34 43 43 10 61

M. Miguel Angel Lopez Herrero
Agence de protection des données
Paseo de la Castellana 41
28046 Madrid
Tél: 00 341 308 47 90
Fax : 00 341 308 46 92

Allemagne

M. J. Jacob, commissaire fédéral à la protection des données représenté par : M. W. von Pommer Esche, chef de département auprès du commissaire fédéral à la protection des données
Riemenschneiderstrasse, 11
53175 Bonn (Bad Godesberg)
Tél : 00 49 228-81995-0
Fax: 00 49 228 81995-50

M. R. Hamm, commissaire du Land de hesse à la protection des données représenté par : Mme A. Schriever-Steinberg, chef du département auprès du commissaire hessois à la protection des données
Uhlandstr, 4
65189 Wiesbaden
Tél : 00 49 611 1408 0
fax : 00 49 611 37 85 79

France

M. A. Türk et Melle F. Fourets
CNIL
rue Saint Guillaume, 21
75340 Paris Cédex 07
Tél : 00 33 1 53 73 22 22
fax : 00 33 1 53 73 22 00

Portugal

M. J.A.M. Labescat da Silva
M. Nuno Albuquerque Morais Sarmento
Rua de S. Bento, 148 3° Andar
1200 Lisbonne
Tél : 00 351 1 39 601 41
Fax: 00 351 1 39 76 832

Luxembourg

M. R. Faber et M. J.P. Reiter, représentants effectifs
Secrétariat de la Commission
Ministère de la Justice 2934 Luxembourg
Tél : 00 352 478 45 46
Fax: 00 352 227 661
M. J. Wagner et M.G. Wivenes, représentants suppléants

Autriche

M^me W. Kotschy
M^me E. Souhrada — Kirchmayer
Ballhausplatz 1
A-1014 Wien
Österreich
Tél: 00 43 1 1531 15/2525 Fax: 00 43 1 53 115/2690

Italie

M. S. Neri
Tél 00 39 6 67 60 46 93
Fax 00 39 95 62 12 20
Fax 00 39 6 676 096 78

M. Buttarelli
Garante per la porfezione dei dati personali
Via della Chiesa Nuova, 8 -00186 Roma
Tél. 00 39 668 18 61
Fax 00 39 668 18 669

Grèce

M. C. Dafermos
Tél. 00 301 779 58 05
Fax 00 30177 80 317
suppléant : M. G. Deliyannis
Tél. 00 301 89 46 451/32 28 056
Fax 00 30177 80 317

Islande : en tant qu'observateur

Mr. S. J.hannesdôttir
Mr. T. Ôrlygsson

Data Protection Commission
Ministry of Justice Armarhvoll
150 Reykjavik — Islande Tél. 00 354
560 90 10 Fax 00 354 552 73 40

Danemark : en tant qu'observateur

Ms. Lotte N. J0rgensen
Registertilsynet
Christians Brygge 28 -1559 K0benhavn V
Danemark
Tél. 00 45 33 14 38 44
Fax 00 45 33 13 38 43

Suède : en tant qu'observateur

Ms. A. Bondestam
General-Director

Ms. B-M. Wester
Administrative Officer
Datainspektionen box 8114
S-104 20 Stockholm — Sweden
Tél. 00 46 8 657 61 00
Fax 00 46 8 650 86 13

Norvège : en tant qu'observateur

M. G. Apenes et Ms. A.M. Bergseng
Postboks 8177 Dep. 0034 Oslo
Tél. 00 47 22 39 69 00
Fax 00 47 22 42 23 50

Finlande : en tant qu'observateur

Head of Finnish delegation : Mr. Aarnio
Ms. J. Meklin (> 9th April 1998)
Ms. Maija Kleemola (<9th April 1998)
Office of the Data Protection Ombudsman
PL 315 Finland 00181 Helsinki
Tél. 00 358 9 18 251
Fax 00 358 9 18 25 7835

Annexe 6
LE DROIT D'ACCÈS ET DE COMMUNICATION DES PERSONNES AUX INFORMATIONS LES CONCERNANT ET INTÉGRÉES DANS LE SYSTÈME D'INFORMATION SCHENGEN

Autorité de contrôle commune Schengen Le

Système d'information Schengen Vous entrez

dans l'espace Schengen

(Pour la Belgique) Commission de la protection de la vie privée Commissie voor de bescherming van de persoonlijke levenssfeer.

(Pour la France) Commission nationale de l'informatique et des libertés.

(Pour le Luxembourg) autorité de contrôle « Système d'information Schengen ».

Le Système d'information Schengen

L'accord de Schengen et sa convention d'application ont créé un espace de libre circulation des personnes en supprimant les contrôles aux frontières intérieures des États membres et en instaurant le principe d'un contrôle unique lors de l'entrée sur le territoire Schengen. Pour des motifs de sécurité, il est cependant apparu nécessaire de mettre en place des mesures compensatoires, au premier rang desquelles figure le Système d'information Schengen (SIS).

Le SIS est un fichier commun à l'ensemble des États membres de l'espace Schengen, qui centralise deux grandes catégories d'informations concernant, l'une, des personnes recherchées ou placées sous surveillance, l'autre, des véhicules ou des objets recherchés.

Par exemple, peuvent être fichées dans le Système d'information Schengen :
- les personnes recherchées ou surveillées par les services de police ;
- les personnes disparues ou qui doivent être placées sous protection, en particulier les mineurs ;
- les personnes non ressortissantes d'un État membre de l'espace Schengen, qui sont interdites d'entrée sur le territoire Schengen ;
- les personnes dont l'identité est frauduleusement utilisée comme alias par d'autres personnes.

Le contrôle du SIS est opéré par une autorité indépendante : l'autorité de contrôle commune Schengen (ACC).

Cette autorité, composée de membres des autorités de protection des données personnelles des États membres de l'espace Schengen, a notamment pour mission, outre d'exercer le contrôle technique du fichier central installé à Strasbourg, de vérifier le respect par les États membres des droits accordés aux personnes par la Convention Schengen.

Vos droits face au SIS

Le SIS vous intéresse directement, que vous soyez ou non ressortissant d'un État membre de l'espace Schengen.

Aussi, des droits particuliers vous sont reconnus par la convention Schengen. Ainsi, vous disposez :

- d'un droit d'accès aux informations vous concernant, enregistrées dans le SIS ;
- d'un droit de rectification lorsque les données sont enregistrées sur la base d'une erreur de droit ou de fait ;
- du droit d'engager une action devant les juridictions ou les instances compétentes pour obtenir la rectification ou l'effacement des informations erronées, ou une indemnisation ;
- du droit de demander une vérification des données enregistrées et de l'utilisation qui en est faite.

Si vous pensez que votre nom figure dans le SIS, n'hésitez pas à exercer vos droits. Les autorités nationales de protection des données des pays membres de l'espace Schengen sont à votre disposition pour vous donner toutes les informations utiles à votre démarche.

Les vérifications sur votre signalement dans le SIS (pertinence de votre inscription dans ce fichier et informations enregistrées à votre sujet) seront effectuées selon le droit national applicable dans le pays que vous choisirez pour exercer vos droits. A votre demande, chaque loi nationale applicable vous sera communiquée par l'autorité nationale de protection des données compétente, dont vous trouverez les coordonnées dans ce dépliant.

Vous serez ensuite informé des résultats obtenus, ou de la suite donnée à votre demande.

Le *Système d'information Schengen vous concerne, ce dépliant est conçu pour répondre à vos questions.*

Consultez-le.

Des organismes officiels sont à votre disposition pour de plus amples informations.

Secrétariat de l'ACC 39,
rue de la Régence 1000
Bruxelles Tél. : 00 322 519 38
76 Fax: 00 322 513 42 06

AUTORITES NATIONALES DE PROTECTION DES DONNEES

Pays-Bas
Registratiekamer
Tel. : 00 31 70 381 13 00
Fax: 00 31 70 381 13 01

Allemagne
Der Bundesbeauffragte fur den Datenschutz
Tél. : 00 49 228 81995-0
Fax: 00 49 228 81995-50

Belgique
Commission de la protection de la vie privée
Commissie voor de bescherming van de persoonlijke levenssfeer
Tél. : 00 32 2 542 72 00
Fax : 00 32 2 542 72 12

Autriche
Datenschutzkommission
Tél. :00 43 1 53 115/2525
Fax: 00 43 1 53 115/2690

Luxembourg
Autorité de contrôle « Système d'information Schengen »
Tél. : 00 352 478 45 62
Fax : 00 352 225 296

France
Commission nationale de l'informatique et des
libertés Tél. : 00 33 1 53 73 22 22
Fax : 00 33 1 53 73 22 00

Portugal
Comisso Nacional de Protecço de Dados Pessoais
Informatizados
Tél. : 00 351 1 392 84 00
Fax: 00 351 1 397 68 32
e mail : cnpdp@imail.telepac.pt

Espagne
Agencia de Proteccion de Datos
Tél.:00349130848 31/3084790
Fax:00349130846 92

Italie
Garante per la protezione dei dati personali
Tél. : 00 39 6 68 18 61
Fax: 00 39 6 68 18 669

Grèce
Autorité de protection des données à caractère personnel
Tél. : 00 301 779 58 05
Fax: 00 301 77 80 317

LES TEXTES DE REFERENCE

- L'accord de Schengen du 14 juin 1985.
- La convention d'application de l'accord de Schengen du 19 juin 1990.

Ces textes vous seront communiqués sur demande par le secrétariat de l'autorité de contrôle commune, dont les coordonnées figurent dans ce dépliant.

Sommaire

Chapitre 2

Chapitre 3

Chapitre 4

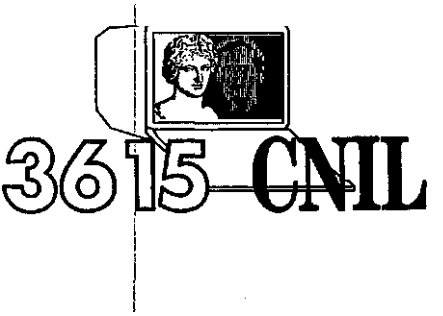
Chapitre 6

Commission nationale de l'informatique et des libertés

21, rue Saint-Guillaume
75340 Paris Cedex 07

Tél. 01 53 73 22 22
Télécopie : 01 53 73 22 00

POUR PLUS D'INFORMATIONS:



Site Internet: http://www.cnil.fr

Imprimé en France par l'imprimerie SAGIM — Dépôt légal : juin 1998 — № d'imprimeur : 2934

18e rapport d'activité 1997

L'année 1997 restera celle d'une prise de conscience de la nécessité de construire une société de l'information respectueuse des règles de protection des données personnelles, tout particulièrement en ce qui concerne Internet.

La Commission nationale de l'informatique et des libertés avait, dès 1995, souligné les risques inhérents à l'utilisation qui pourrait être faite du gisement de données personnelles que constitue Internet. En 1996, la CNIL avait appelé l'attention sur le phénomène de la traça-bilité des données relatives aux internautes qui naviguent sur le web.

Les travaux de la Commission sur ces questions se sont depuis lors considérablement enrichis, notamment en ce qui concerne l'ouverture de sites ministériels sur Internet, le développement du commerce électronique ou les traitements d'informations nominatives mis en oeuvre par les fournisseurs d'accès au réseau.

Les interventions et réflexions de la CNIL concernant Internet et les flux transfrontières d'informations nominatives s'inscrivent dans un contexte national et un environnement international en pleine mutation.

Ce rapport rend ainsi compte de la poursuite des travaux liés à la transposition en droit français de la directive européenne du 24 octobre 1995 en présentant les suggestions faites par la CNIL au gouvernement à cet égard.

Ce 18e rapport d'activité dresse par ailleurs le bilan des autres activités de la CNIL, en ce qui concerne tant l'examen des fichiers informatiques avant leur mise en oeuvre -près de 70.000 dossiers de formalités préalables ont été enregistrés cette année par la Commission- que le contrôle a *posteriori* de ces fichiers à travers l'instruction des plaintes, l'exercice du droit d'accès indirect -dont le nombre de demandes a augmenté de plus de 20% ou les visites sur place.

Parmi les questions évoquées dans ce rapport, les recommandations et les avis émis par la CNIL à propos des mégabases de données comportementales, des annuaires téléphoniques de nouvelle génération (annuaires inverses ou accessibles par Internet) ou encore de la montée en charge du dispositif Sesam-Vitale, attestent que l'informatique peut demeurer au service de chaque citoyen et qu'il est toujours possible de conjuguer progrès technique et liberté.

Retrouvez la CNIL sur Internet : http://www.cnil.fr.

Prix : 190 F
La Documentation française
29-31, quai Voltaire
75344 Paris Cedex 07
Imprimé en France
ISBN: 2-11-004033-5
DF : 54699-2