23e rapport d'activité 2002

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Édition 2003

La **documentation** Française

CNIL

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

23e rapport d'activité 2002

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

ISBN 2-11-005434-4

Sommaire

L'évolution permanente des techniques d'information et de communication oblige la Commission nationale de l'informatique et des libertés à avoir le regard rivé sur l'horizon mouvant d'un monde informatique qui, par ses contours vertigineux, n'est pas sans ressemblance avec la bibliothèque de Babel telle que la décrit Borges : *« un nombre indéfini et peut-être infini de galeries hexagonales avec au centre de vastes puits d'aération bordés par des balustrades très basses ».* C'est pourtant vers le proche passé que le législateur demande à la CNIL de se retourner en lui imposant l'exercice salutaire du rapport annuel. Salutaire parce que la CNIL, autorité administrative indépendante, doit rendre compte de son action aux autorités de l'État, au Parlement et à l'opinion. Salutaire aussi parce qu'il incite nécessairement à la modestie.

Le chapitre préliminaire de ce rapport est bien le compte rendu de la vie quotidienne d'un organisme qui est à la fois un « guichet » où s'accomplissent les formalités préalables à la mise en œuvre des traitements de données personnelles et où sont reçues des plaintes mais aussi un lieu de débats et de réflexion. Ce chapitre fait d'abord ressortir la forte progression du nombre de plaintes et de demandes d'accès aux fichiers de police et de sécurité publique. À travers ces « saisines » s'établit un lien direct avec les citoyens français ou étrangers qui attendent l'appui ou le secours de la CNIL face à des organismes publics et privés souvent opaques. C'est pourquoi chacun des chapitres de la première partie « Au cœur de l'activité 2002 » s'efforce de montrer, à travers des cas réels, comment la CNIL intervient concrètement pour résoudre les problèmes qui lui sont soumis.

Le deuxième trait saillant, tout le rapport en témoigne, ne surprendra pas : c'est le fait que l'activité européenne et internationale de la CNIL est devenue une dimension essentielle de son action tant il est avéré que la protection des données ne peut être assurée pleinement si elle ne l'est qu'à l'intérieur de nos frontières. La CNIL, si elle cherche tous les relais possibles chez ses homologues ou dans les organisations internationales, n'en milite pas moins pour que le droit national français ou le droit européen unifié par la directive d'octobre 1995 soit considéré comme applicable à des opérations de collecte de données effectuées en France par des sites web établis hors de l'Union européenne ainsi que cela est exposé au chapitre 4.

Un troisième élément à mettre en avant résulte entièrement de la volonté de la CNIL d'infléchir ses modes d'intervention : la multiplication des décisions de contrôle sur place. Cette démarche est souvent menée plus dans une optique d'information que d'investigation. Mais elle débouche aussi sur des dénonciations au procureur de la République d'infractions pénales à la législation « Informatique et libertés ». À cet égard il faut souligner que 2002 restera comme l'année du nombre record de dénonciations au parquet : sept en une seule année contre dix-huit seulement dans les vingt-trois années précédentes d'application de la loi du 6 janvier 1978.

Une bonne part de ces dénonciations est le fruit d'une opération emblématique dirigée contre les courriers électroniques non sollicités : « la boîte à spams » qui est largement évoquée au sein du chapitre 2, consacré aux mutations, parfois périlleuses pour notre vie privée et notre tranquillité, de la prospection commerciale. Cette opération traduit le souci de la CNIL de se mobiliser sur des sujets qui concernent la vie quotidienne des gens, ici des internautes, autrement dit bientôt chacun de nous. La banalisation de l'usage d'internet permet d'écrire ce mot sans sa majuscule. Elle ne met pas fin aux inquiétudes légitimes que ses usagers peuvent nourrir sur la confidentialité des données personnelles qui sont mises en circulation universelle. Le chapitre 5 expose les réponses pragmatiques qu'apporte la CNIL.

Y a-t-il matière à dénoncer une frilosité de la CNIL à l'égard de la « société de l'information » ? C'est le procès dont la menacent les tenants d'une généralisation à marche forcée du vote électronique. Sans aucun attachement nostalgique au préau d'école et à l'urne en bois, la CNIL a eu plusieurs occasions au cours de l'année 2002, année électorale s'il en fut, de préciser les garanties qui doivent selon elle entourer ces scrutins dématérialisés pour qu'ils ne soient pas démonétisés (chapitre 3).

La CNIL est bien placée pour constater que l'informatisation de la société ne passe pas uniquement par internet. L'année 2002 a montré que l'encadrement des grandes bases de données nominatives reste un enjeu de taille. C'est ainsi qu'elle a été amenée à se prononcer sur l'extension des fichiers de police judiciaire réalisée par la loi sur la sécurité intérieure (chapitre 1), sur le nouveau recensement (chapitre 7) ou encore sur les outils du pilotage de la santé publique (chapitre 6). La CNIL est dans sa mission classique mais toujours d'actualité de modérateur de l'exercice des fonctions régaliennes de l'Etat. Lorsque des bases de données conditionnent des actes plus banals, obtenir un crédit, souscrire un abonnement téléphonique (chapitre 5), faire connaître son numéro de téléphone ou sa nouvelle adresse (chapitre 7), la CNIL se voit investie, en plus de celui de régulation, d'un rôle de médiation qu'elle remplit dans un esprit de service au public.

Parmi tous les événements qui ont marqué la vie de la CNIL en 2002, il en est un, pourtant majeur, qui n'est pas évoqué dans le présent rapport : le vote par l'Assemblée nationale le 30 janvier 2002 du projet de loi transposant la directive européenne sur la protection des données et modifiant la loi du 6 janvier 1978. Avec cet acte législatif, un pas décisif est franchi : le premier. Toutefois le calendrier électoral et parlementaire n'a pas permis d'aller plus loin au cours de l'année 2002. Puisse l'année 2003 dont le premier trimestre a vu le Sénat adopter à son tour le projet en première lecture être celle de l'achèvement de ce processus indispensable.

Michel GENTOT

LA CNIL EN CHIFFRES ET EN PRATIQUE

I. LA CNIL AU QUOTIDIEN

Intense et multiforme, l'activité de la CNIL est le reflet de la diversité des missions qui lui sont dévolues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

A. Séances plénières

À la fois organe délibérant et lieu de réflexion, la Commission se réunit en séance plénière deux fois par mois sur un ordre du jour établi à l'initiative de son président, M. Michel Gentot (cf. annexe 1 Composition de la Commission).

Lors de ces séances plénières, la Commission adopte des délibérations -1 1 1 en 2002 (cf. annexe 4 Liste des délibérations) — qui sont soit des avis sur des traitements ou des fichiers, soit des suites données à des plaintes, des demandes de conseil ou à des contrôles.

Dans ce dernier cadre, il arrive que la CNIL, en vertu de l'article 21 -3^{e} de la loi du 6 janvier 1978, adresse des avertissements ou dénonce des affaires à la justice. Ainsi en 2002, la Commission a délivré deux avertissements et a transmis au parquet sept dossiers, ce qui a porté à vingt-cinq le nombre de dénonciations au parquet effectuées depuis sa création (cf. *infra* chapitres 2 et 3).

Enfin, nombre de rapports font le point sur les évolutions de l'informatique afin d'éclairer les membres de la CNIL dans la conduite de leurs missions. Parmi les sujets traités en 2002 on relèvera l'identité numérique, la signature électronique, l'administration électronique...

La CNIL peut aussi procéder, soit de sa propre initiative, soit à la demande des personnes concernées, à des auditions en séance plénière. Au cours de l'année 2002, la CNIL a ainsi entendu M. Martin Vial, président de La Poste, sur les implications de certains projets de ce groupe au regard de la loi « Informatique et libertés » et M. Jacques Sauret, directeur du GIP « Modernisation des déclarations sociales », à propos du portail net-entreprises (cf. chapitre 7).

Compte tenu de la grande variété des dossiers que la CNIL doit traiter, une répartition par secteur d'activité est établie entre les commissaires (cf. annexe 2 Répartition par secteur d'activité). Cette répartition a l'avantage d'instaurer une forme de spécialisation et de faciliter les contacts des commissaires avec les responsables de traitements. Néanmoins, les délibérations de la CNIL sont débattues selon les principes de la collégialité.

B. Activités hors séances plénières

Pour conduire leurs missions, les membres de la CNIL s'appuient sur différents services, soit quatre-vingts agents répartis au sein de trois directions : juridique, administrative et, c'est une spécificité de la CNIL, de l'expertise informatique et des contrôles (*cf.* annexe 3 Organisation des services).

Investie d'une mission générale de réflexion prospective, la Commission a créé en son sein divers groupes de travail, notamment sur le blanchiment d'argent au sein d'établissements de crédit, les listes noires ou encore l'administration électronique.

Dans ce dernier domaine, la CNIL qui reçoit et traite des milliers de déclarations au titre des formalités préalables à la mise en oeuvre des traitements de données personnelles ne peut se contenter d'observer et de conseiller les autres administrations. Il lui revient de prendre sa part au chantier de la simplification des relations avec les usagers. C'est pourquoi, après avoir proposé sur son site www.cnil.fr un module de télédéclaration de sites internet, la Commission offre depuis la fin de l'année 2002 la possibilité de déclarer en ligne les fichiers les plus courants (« télédéclaration simplifiée »).

Au-delà de ses activités de recensement et de contrôle des fichiers, des réponses faites aux demandes de conseil et de l'instruction des plaintes, la CNIL consacre, conformément à ses missions, une partie de son activité à l'information des personnes sur leurs droits et sur leurs obligations. Directement sollicitée par de nombreux organismes, sociétés ou institutions pour conduire des actions de formation et de sensibilisation à la loi « Informatique et libertés », la CNIL participe aussi à des colloques, des salons ou des conférences pour informer et en même temps s'informer. A titre d'exemple, la CNIL a pris part en 2002 au salon des collectivités locales afin d'aller directement à la rencontre des élus et des administrateurs territoriaux pour mieux leur faire connaître leurs obligations. Au final, c'est à près de 250 manifestations, réunions ou colloques auxquels la Commission a collaboré au cours de cette même année, pour l'essentiel en tant qu'intervenant.

Pour donner plus d'écho à certaines de ses décisions ou de ses actions, la CNIL publie régulièrement des communiqués de presse ou, plus rarement, organise des conférences de presse. Les sujets abordés dans ce cadre en 2002 ont concerné par exemple les informations collectées à l'occasion d'un recrutement, la lutte contre le « spam », les techniques biométriques de contrôle, la cybersurveillance des travailleurs ou encore les mineurs et internet, thèmes qui sont d'ailleurs au cœur de l'activité de la CNIL depuis plusieurs années. La conférence de presse au cours de laquelle la CNIL a exposé sa position sur le projet de loi de sécurité intérieure *(cf.* chapitre 1) a suscité un vif intérêt de la part des journalistes.

C. Activités européennes et internationales

La coopération européenne et internationale en matière de protection des données personnelles est devenue, sous l'effet conjugué de l'intégration européenne et de la mondialisation des échanges, une réalité quotidienne. La CNIL fait partie d'un réseau constitué de ses homologues en Europe et au-delà.

Il ne se passe guère de jour qu'elle ne reçoive une demande d'information sur la pratique française. À son tour, la CNIL trouve un relais précieux chez les autorités de contrôle étrangères pour traiter les plaintes « extraterritoriales » ou « transfrontalières » qui sont en nette augmentation.

L'entrée dans ce cercle des autorités des dix pays d'Europe centrale et orientale retenus pour l'élargissement en 2004 de l'Union européenne est un enjeu de première importance qui a conduit la CNIL à réaliser des actions de coopération bilatérale avec la Pologne ou la Slovaquie et à participer aux conférences organisées par la Commission européenne ou le Conseil de l'Europe (conférence de Madrid, décembre) à l'intention de ces pays.

La CNIL assiste bien entendu aux deux conférences des commissaires à la protection des données qui se tiennent annuellement (conférence des commissaires européens à Bonn en avril 2002, conférence internationale à Cardiff en septembre 2002). En outre, la conférence européenne a créé un groupe de travail sur les plaintes transfrontalières. Enfin la CNIL participe au groupe de travail international sur la protection des données dans le secteur des télécommunications.

Toutefois c'est à Bruxelles, au sein des instances européennes instituées dans le domaine de la protection des données, que sont menés les travaux les plus significatifs car les plus normatifs.

1. LE GROUPE DE « L'ARTICLE 29 »

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité nationale. Le groupe a pour mission de contribuer à l'élaboration des normes européennes par ses recommandations destinées à l'application homogène de la directive dans l'Union européenne, ses avis sur le

niveau de protection dans les pays tiers et ses conseils à la Commission sur tout projet de mesure ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles.

Ce groupe dit « de l'article 29 », présidé par M. Rodota, président de l'autorité italienne de protection des données, s'est réuni quatre fois au cours de l'année 2002 en session plénière d'une ou deux journées et s'est appuyé sur des sous-groupes de travail notamment « secteur emploi », « droit national », « clauses contractuelles types et transferts de données vers des pays fiers » et « *Task Force Internet ».*

Les recommandations les plus importantes adoptées en 2002 ont concerné un avis positif sur le niveau de protection des données en Argentine, le suivi de l'accord *« Safe Harbor »* aux États-Unis, la question des transmissions des informations détenues par les compagnies aériennes aux douanes américaines *[cf.* chapitre 1), le droit national applicable aux sites web dont les responsables sont établis dans les pays tiers *(cf.* chapitre 4), les services d'authentification en ligne, la videosurveillance, les listes noires, la surveillance électronique des salariés sur leur lieu de travail, le protocole IPV6 et l'identifiant des terminaux.

La CNIL siège aussi au sein de trois autorités de contrôle communes (ACC) Europol, Schengen et Eurodac, dont la mission consiste à garantir la protection des droits des citoyens face aux traitements automatisés à caractère policier mis en œuvre dans le cadre de chacune des conventions ou règlements applicables.

2. L'AUTORITE DE CONTROLE COMMUNE EUROPOL

En 2002, l'autorité de contrôle commune (ACC) Europol, présidée par M. Alex Türk, vice-président de la CNIL, puis depuis le 1er décembre 2002 par M. Klaus Kalk, membre de la délégation allemande, s'est réunie à cinq reprises en session plénière. Deux sujets majeurs ont particulièrement retenu l'attention de l'ACC Europol au cours de l'année 2002 : les relations développées par Europol avec les États-Unis d'Amérique à la suite des événements du 11 septembre 2001 *(cf. infra* chapitre 1) et la proposition danoise en date du 2 juillet 2002 visant à modifier la Convention Europol dont l'examen se poursuit en 2003 compte tenu des nouvelles modifications apportées au projet de texte postérieurement à l'avis de l'autorité.

Parallèlement à ces questions qui revêtent toutes deux un caractère exceptionnel, l'ACC a rempli les missions qui lui sont confiées aux termes de la Convention Europol du 26 juillet 1995. Ainsi, l'ACC a rendu des avis sur sept nouveaux projets d'ouverture de fichiers d'analyse. Elle a en outre rendu des avis en application de l'article 18 de la Convention et de l'acte du Conseil du 12 mars 1999 arrêtant les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers, concernant la possibilité pour le directeur d'Europol soit d'engager des négociations, soit de conclure un accord en ce sens avec divers États.

Dans le prolongement de ces négociations, l'ACC a jugé utile au mois de juin 2002 d'organiser une réunion avec les autorités nationales de protection des données des pays et organes tiers avec lesquels Europol a conclu un accord. Cette

première rencontre, qui s'est déroulée en présence de représentants des autorités tchèque, slovaque, polonaise, estonienne, norvégienne et d'Interpol, a permis de poser les jalons d'une coopération entre l'ACC et ces-autorités nationales de protection des données.

Sur un plan plus technique, l'ACC a émis des avis sur les moyens informatiques mis en œuvre par Europol, plus particulièrement le nouveau système d'analyse et le système d'index, et a procédé au mois de mars 2002 à une deuxième inspection auprès d'Europol. Le comité des recours, quant à lui, s'est réuni selon la même périodicité que l'ACC et a rendu en séance publique, le 16 mai 2002, sa première décision.

3. L'AUTORITE DE CONTRÔLE COMMUNE SCHENGEN

L'autorité de contrôle commune (ACC) Schengen, présidée par M. Giovanni Buttarelli, membre de la délégation italienne, s'est réunie cinq fois en 2002. Ce sont les projets de modification de la Convention d'application de l'accord de Schengen du 19 juin 1990 et du système d'information Schengen (SIS) présentés par la présidence espagnole qui ont été les principaux sujets d'intérêts de l'ACC durant l'année 2002. Ces projets visent à conférer au SIS II de nouvelles fonctionnalités, à prévoir l'enregistrement de données supplémentaires, et à autoriser la consultation du SIS par de nouveaux destinataires, en particulier Europol et Eurojust. L'adoption de ces modifications conduirait à changer fondamentalement la nature du SIS qui, système permettant d'exécuter des signalements, deviendrait un système d'information susceptible d'être plus largement utilisé dans le cadre de la coopération européenne policière et judiciaire.

4. L'AUTORITÉ DE CONTROLE COMMUNE EURODAC

Eurodac, créé par le règlement du Conseil de l'Union européenne du 11 décembre 2000, a pour objet de permettre aux autorités habilitées[1] des États membres de l'Union européenne (à l'exception du Danemark), et aux pays tiers parties au règlement (la Norvège et l'Islande), de procéder aux comparaisons des empreintes digitales de trois catégories de ressortissants étrangers âgés de plus de 14 ans :

— les demandeurs d'asile afin de déterminer, selon le mécanisme prévu par la Con vention de Dublin du 15 juin 1990, l'État responsable de l'examen d'une demande d'asile présentée dans l'un des États membres, ainsi que les modalités de prise en charge du demandeur ;

— les étrangers appréhendés à l'occasion du franchissement irrégulier d'une fron tière extérieure ;

— les étrangers se trouvant illégalement sur le territoire d'un État membre.

[1] Il s'agit en France du ministère de l'Intérieur et de l'Office français de protection des réfugiés et apatrides (OFPRA).

Ce système européen, opérationnel depuis le 15 janvier 2003, est installé à Luxembourg. Il est composé d'une base de données centrale placée sous l'autorité de la Commission européenne et de moyens électroniques de transmission entre les États et la base commune.

Outre les empreintes digitales, les informations transmises par les Etats sont le sexe de la personne concernée, un numéro de référence, et le cas échéant le lieu et la date de demande d'asile. Eurodac traitant des informations indirectement nominatives (le numéro permettant de faire le lien entre les empreintes digitales enregistrées et leur titulaire), son fonctionnement est placé sous la surveillance d'une autorité de contrôle commune (ACC) indépendante, composée de représentants des autorités de contrôles nationales des États membres.

Cette nouvelle autorité, à laquelle se substituera le contrôleur européen de la protection des données personnelles prévu par l'article 286 du traité sur l'Union européenne lorsqu'il sera installé, a tenu sa première réunion le 28 novembre 2002. L'ACC a procédé à l'élection de son président, M. Alex T-RK, vice-président de la CNIL, et a adopté son règlement intérieur.

II. LES SAISINES EN FORTE AUGMENTATION

Les articles 6, 21, 22 et 39 de la loi du 6 janvier 19p78 confient à la CNIL la mission d'informer les personnes de leurs droits et obligations, de tenir à leur disposition le registre des traitements déclarés (« fichier des fichiers »), de recevoir les réclamations, pétitions et plaintes ainsi que d'exercer, à la demande des requérants, le droit d'accès aux fichiers intéressant la sécurité publique et la sûreté de l'État.

En 2002, tous les chiffres relatifs aux saisines de la CNIL sont en hausse. La Commission a enregistré une véritable explosion :

— des demandes d'accès indirect aux fichiers de police et de sécurité publique de + 51 %, et ce malgré la croissance des années précédentes, de + 67 % en 1999, + 21 % en 2000, + 2,4 % en 2001 (cf. chapitre 1 point II) ;

— des plaintes de + 42 %, progression qui suit un doublement de leur nombre entre 2000 et 2001.

Ces augmentations sans précédent prouvent l'attachement de nos concitoyens aux droits que leur *confère* la loi « Informatique et libertés » et le fait qu'ils n'hésitent pas à dénoncer les abus dont ils sont ou pensent être victimes. Enfin, le net accroissement des demandes d'extrait du « fichier des fichiers » de + 32 % illustre là encore le souci des citoyens de connaître l'utilisation des données qui les concernent.

À titre de rappel, la CNIL a reçu depuis 1978 plus de 12 600 demandes de conseil et plus de 41 270 plaintes (au 31 décembre 2002).

Les demandes de conseil portent le plus fréquemment sur les formalités préalables à la mise en oeuvre des fichiers. En 2002, les secteurs d'activité qui ont suscité

le nombre le plus important de demandes de conseil sont, par ordre décroissant : travail, santé, fiscalité, collectivités locales.

L'objet le plus fréquent des plaintes concerne l'exercice des droits et tout particulièrement du droit d'opposition à figurer dans un traitement ou à faire l'objet de prospection commerciale. Les secteurs d'activité qui ont suscité en 2002 le nombre le plus important de plaintes sont, par ordre décroissant : prospection commerciale *[cf.* chapitre 2), banque *[cf.* chapitre 5), travail, télécommunications *[cf.* chapitre 5).

Nature des saisines	**1995**	**1996**	**1997**	**1998**	**1999**	2000	2001	2002	**Variation 2001 /2002**
Demandes de droit d'accès indirect	243	320	385	401	671	817	836	**1 264**	**+ 51** %
Plaintes	1 636	2 028	2 348	2 671	3 508	3 399	3 574	**5 076**	**+ 42** %
Demandes de conseil	985	1 008	821	1 115	1 061	1 049	973	**1 126**	**+ 16 %**
Demandes de radiation des fichiers commerciaux	263	277	263	204	186	144	94	**110**	+ **17** %
Demandes d'extraits du fichier des fichiers	122	170	155	154	133	208	252	**333**	**+ 32** %
Total	**3 249**	**3 803**	**3 972**	**4 545**	**5 559**	**5 617**	**5 729**	**7 909**	**+ 38** %

III. LA MULTIPLICATION DES DECISIONS DE CONTRÔLE

Le nombre de contrôles décidés par la CNIL en 2002 s'élève à cinquante-deux. Ce nombre, qui est deux fois plus important que les années précédentes, marque la volonté d'anticiper la transposition en droit interne de la directive européenne 95/46 du 24 octobre 1995[1] qui conduira la CNIL à mettre de plus en plus l'accent sur le contrôle a *posteriori.*

[1] Le projet de loi assurant cette transposition a été discuté en première lecture par l'Assemblée nationale en janvier 2002, peu avant l'interruption des travaux du Parlement et la fin de la onzième législature. Le Sénat ne l'a examiné, en première lecture, qu'en 2003.

Parmi la trentaine de missions de contrôle effectuées cette année, on relèvera que la mission effectuée auprès des sociétés Impact Net *(cf.* chapitre 3), qui a procédé entre les deux tours de l'élection présidentielle à un sondage politique par internet, et Clara Net (hébergeur) a conduit la CNIL à dénoncer au parquet les faits constatés (en particulier la constitution d'un traitement indirectement nominatif en l'absence de toute formalité auprès de la CNIL et la collecte d'informations relevant de l'article 31 de la loi sans que soit recueilli le consentement exprès des intéressés).

Dans les autres cas, la Commission a rappelé aux responsables des organismes concernés (une société spécialisée en équipements automobiles et un réseau de grande distribution au sujet de la gestion de leurs salariés, une mairie de la région parisienne concernant les inscriptions scolaires, un établissement bancaire pour le démarchage commercial par internet de ses clients) l'obligation de respecter la loi du 6 janvier 1978.

Plusieurs séries de missions de contrôles ont été effectuées dans le cadre d'études menées par la Commission :

Les travaux du groupe de travail sur les fichiers de personnes à risques ou « listes noires » ont été enrichis par une série de missions de contrôle auprès des principaux loueurs de véhicules (Avis, Hertz, Europcar, Ada, Budget, Rent-a-Car) et de leur chambre syndicale, le Conseil national des professions de l'automobile. Une recommandation relative à la gestion de fichiers de personnes à risques par les loueurs de véhicules a été adoptée par la Commission le 11 mars 2003.

À la suite de l'adoption en février 2002 du rapport sur la cybersurveillance, plusieurs missions ont été effectuées afin de vérifier les modalités de mises en œuvre des recommandations de la Commission en la matière par des sociétés du secteur privé ou des administrations. La Commission devrait tirer les enseignements de ces missions en 2003.

L'examen de l'application NAVIGO de la RATP a conduit la CNIL à procéder à des investigations auprès de sociétés de transport en commun — implantées à Amiens, Lyon, Valenciennes, Marseille et Nice — qui ont mis en œuvre des systèmes de télébilletique, afin de vérifier notamment les durées de conservation des données enregistrées à l'occasion des déplacements des usagers. Une recommandation relative à la collecte et au traitement d'informations nominatives par les sociétés de transport en commun dans le cadre des applications billettiques devrait être adoptée par la Commission courant 2003.

IV. LES FORMALITES PREALABLES À LA MISE EN ŒUVRE DES FICHIERS

Au 31 décembre 2002, le nombre de traitements enregistrés par la CNIL depuis 1978 était de 875 1*55.*

	1978-2002	% du total des formalités
Déclarations simplifiées	599 843	65,60 %
Demandes d'avis	48 963	5,40 %
Déclarations ordinaires	199 829	21,80 %
Déclarations sites internet (depuis 1997)	24 628	2,70 %
Demandes d'autorisation (chap. V^{bis} — depuis 1997)	**1** 688	0,18 %
Demandes d'autorisation (chap. V^{ler} — depuis 1999)	204	0,02 %
Total des traitements enregistrés	**875 155**	—
Déclarations de modification	38 621	4,30 %
Total des formalités préalables	**913 776**	100,00 %

Entre le 1er janvier et le 31 décembre 2002, la CNIL a enregistré 54 128 nouveaux dossiers de formalités préalables et 2 915 déclarations de modification de traitements déjà enregistrés.

Il convient de noter un léger infléchissement du nombre de demandes d'avis émanant du secteur public (- 3 *%)* et une nette baisse des déclarations ordinaires émanant du secteur privé (-42 *%).* Cette baisse paraît révéler un certain attentisme des déclarants du secteur privé qui anticipent sur l'allégement des formalités déclaratives attendu de la transposition en droit interne de la directive européenne 95/46. En revanche, le nombre de déclarations simplifiées concernant les traitements les plus courants connaît une reprise de + 11 % qui peut s'expliquer par les facilités de déclaration offertes à présent sur le site de la CNIL (téléchargement des formulaires et déclaration en ligne).

Après avoir progressé d'année en année, le nombre de déclarations de sites internet se stabilise. Ce sont en tout 24 628 sites internet qui étaient recensés à la CNIL au 31 décembre 2002. La liste de ces sites déclarés est accessible directement à partir du site www.cnil.fr dans la rubrique « Sites déclarés ».

	1997	1998	1999	2000	2001	**2002**	Variation 2001 /2002
Déclarations simplifiées	53 953	50 735	43 571	33 657	29 755	**33 261**	+11 %
Demandes d'avis	2 724	3 002	3 538	3 577	3 868	**3 733**	- 3 %
Déclarations ordinaires	10 326	11 333	12 200	15 249	16 119	**9 320**	- 42 %
Déclarations sites internet (depuis 1997)	267	930	2 562	6 114	7 389	**7 366**	- 0,3 %
Demandes d'autorisation (chap. V^{bis} — depuis 1997)	133	244	352	287	288	384	+ 33 %
Demandes d'autorisation (chap. V^{ter} — depuis 1999)	—	—	8	73	59	**64**	+ 8 %
Déclarations de modification	2 639	2 358	**3** 454	**2** 607	3061	**2915**	-4 %
Totaux	**70 042**	**68 602**	**65 685**	**61 564**	**60 539**	**57 043**	**- 5 %**

V. LA SUITE DES GRANDS DOSSIERS DE L'ANNÉE 2001

La CNIL ne clôt pas chaque 31 décembre les grands dossiers qui l'ont mobilisée au cours d'une année. C'est le cas de deux thèmes forts de l'année 2001.

A. L'administration électronique

Dans son rapport d'activité pour l'année 2001, la Commission, après avoir rappelé l'intérêt qu'elle porte au développement de l'administration électronique comme en témoignent les nombreux avis favorables déjà rendus sur les téléprocédures dont elle a été saisie, avait fait part de ses réflexions sur les enjeux que soulève, selon elle, cette nouvelle forme d'administration.

Tout en rappelant que l'administration électronique devait nécessairement se traduire par une simplification des démarches administratives et, plus fondamentalement, de la règle de droit, la Commission avait insisté sur un certain nombre de lignes directrices qui doivent selon elle guider les projets de réformes en ce domaine : le respect du principe d'égalité devant le service public, la sectorisation des identifiants (que l'on peut exprimer par la formule « à chaque sphère son identifiant »), les exigences de confidentialité ou encore le principe de transparence, l'administration électronique apparaissant comme une singulière opportunité pour permettre à l'usager d'exercer pleinement les droits qui lui sont reconnus en particulier par la loi de 1978 et notamment un droit d'accès en ligne.

En 2002, la Commission, outre les projets spécifiques de téléprocédures qui lui ont été soumis pour avis (cf. chapitre 7, IV), a suivi avec une attention particulière les travaux du Gouvernement sur l'administration électronique. Elle a ainsi été associée aux groupes de travail mis en place par la direction interministérielle à la réforme de l'État (DIRE) en particulier sur le projet de portail (monservicepublic. fr), sur le service de changement d'adresse ou, encore, sur les projets de carte de vie quotidienne au sein des collectivités locales. Ces chantiers s'inscrivent dans le plan d'action gouvernemental pour la société de l'information lancé par le Premier ministre, M. Jean-Pierre Raffarin (programme RE-SO, 2007). Afin de poursuivre sa réflexion sur le sujet et faire œuvre de proposition, la CNIL a mis en place, en son sein, un groupe de travail qui suit très attentivement l'avancement de ces projets.

La fin de l'année 2002 a été marquée par la publication du rapport de M. Pierre de la Coste intitulé *L'hyper-république* qui a tenté d'esquisser les perspectives de l'administration électronique en France. Il est regrettable que les questions de protection des données personnelles soient peu évoquées dans le rapport et quand elles le sont, sous un angle plutôt critique, comme un point de blocage de l'administration électronique. Le Forum des droits sur l'internet, de son côté, a rendu publiques, peu de temps après, ses pistes de réflexion sur le développement de l'administration électronique qui, pour une large part, rejoignent les recommandations exprimées par la CNIL en 2001.

Par ailleurs à l'initiative des représentants de la CNIL au sein du groupe dit de « l'article 29 », un état des lieux sur l'administration électronique et la protection des données personnelles a été réalisé sur la base d'un questionnaire auquel les autorités des pays de l'Union européenne étaient invitées à répondre. Celui-ci a porté sur l'implication des autorités de protection des données, le développement des téléservices et les principales problématiques relatives à la protection des données. La synthèse des réponses est présentée en annexe à ce rapport *(cf.* annexe 7 Groupe article 29).

B. La cybersurveillance des salariés

La cybersurveillance sur les lieux de travail reste un sujet de préoccupation, comme en témoignent les plaintes et demandes de conseil que la CNIL reçoit quotidiennement sur la question. La Commission, après avoir procédé à une étude d'ensemble sur le sujet et en particulier réalisé une consultation publique, a fait part de ses conclusions et de ses recommandations pratiques dans un rapport présenté par M. Hubert Bouchet, vice-président de la Commission et adopté le 5 février 2002[1].

À cet égard, il est satisfaisant de constater que les chartes d'utilisation des outils informatiques dont la CNIL est saisie tiennent de plus en plus compte de ces recommandations. Au-delà de ce constat encourageant, la CNIL a souhaité poursuivre son travail de pédagogie et s'assurer sur le terrain des suites données à ses recommandations en matière de cybersurveillance et, comme cela a été indiqué plus haut, a conduit plusieurs missions d'information sur ce thème.

En outre, en vue de contribuer à l'application homogène de la directive 95/46/CE le groupe européen dit de « l'article 29 » s'est attaché en 2002 à fournir des orientations communes en matière de cybersurveillance des salariés. Le document de travail adopté le 29 mai 2002 s'inspire largement des recommandations de la CNIL ainsi que de celles très convergentes des autorités des Pays-Bas et du Royaume-Uni dont les travaux avaient reçu une large audience également dans leur pays.

Ainsi, le groupe, en constatant qu'il serait irréaliste de priver les salariés de tout usage personnel des moyens informatiques mis à leur disposition par l'entreprise et en relevant le caractère illégal de l'exercice d'un contrôle sur le contenu des messages privés échangés, s'est efforcé de formuler des conseils pratiques à l'adresse des employeurs dans leur tâche légitime de surveillance du travail. Ces conseils pratiques visent la transparence et la proportionnalité des mesures mises en œuvre en ce qui concerne l'usage de la messagerie électronique et de l'accès aux sites d'information. Ils tiennent naturellement compte des impératifs de sécurité des systèmes d'information.

---

[1] *Cf.* 21e rapport d'activité de la CNIL, p. 121, et 22e rapport d'activité, p. 54.
Les rapports « cybersurveillance » adoptés par la CNIL sont également disponibles sur www.cnil.fr

PREMIER PARTIE

AU CŒUR DE L'ACTIVITÉ 2002

Chapitre 1

SÉCURITÉ INTERIEURE, FICHIERS ET LIBERTÉS

Personne ne s'étonnera que la sécurité intérieure soit inscrite en tête de cette partie du rapport consacrée aux dossiers qui ont marqué l'activité de la CNIL en 2002. Certes 2002 a été l'année des élections présidentielle et législative et le thème de la cyberdémocratie aurait pu aussi être mis en exergue. Mais précisément la sécurité intérieure, préoccupation forte des Français, a été au centre de ces campagnes électorales et a ensuite absorbé une partie des travaux parlementaires de la nouvelle législature. De plus, il est clair que pour la CNIL l'enjeu est majeur. Le contrôle des fichiers de police est en effet « une pierre de touche » de l'effectivité du rôle joué par la Commission en tant qu'autorité administrative indépendante chargée de la protection des données nominatives ainsi que du respect par l'État du principe fondamental du droit des personnes à cette protection.

Obtenir un encadrement des modalités de fonctionnement des fichiers de police dans des conditions qui assurent un équilibre satisfaisant entre la liberté individuelle et l'efficacité des enquêtes, tel a été l'objectif de la CNIL dans sa participation au débat public sur le projet de loi de sécurité intérieure. Surveiller l'usage de ces fichiers en donnant aux individus, autant que la sécurité publique le permet, un accès aux informations détenues sur eux, c'est le lot quotidien des membres de la CNIL qui sont plus spécialement investis de cette mission et qui ont à faire face à un flot croissant de demandes.

La dimension européenne et internationale ne saurait être absente de ce chapitre : à l'évidence la sécurité est une préoccupation qui dépasse les frontières mais surtout qui conduit à les faire traverser par de nombreux flux de données personnelles.

I. LA LOI SUR LA SECURITE INTERIEURE

Le 23 octobre 2002, M. Nicolas Sarkozy, ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales a présenté en Conseil des ministres le projet de loi pour la sécurité intérieure qui, entre autres, comportait un chapitre intitulé « Dispositions relatives aux traitements automatisés d'informations » et ayant pour objet les fichiers de police judiciaire. Un autre chapitre, « Dispositions relatives aux moyens de police technique et scientifique », prévoyait une extension importante du fichier national automatisé des empreintes génétiques (FNAEG).

Le même jour, la CNIL qui n'avait pas été consultée sur le projet de loi a jugé nécessaire de faire connaître sa position au Gouvernement et au Parlement, au moment précisément où la discussion s'ouvrait à l'Assemblée nationale. C'est la première fois dans l'histoire de la CNIL que celle-ci se saisissait d'office d'un projet de loi.

La loi pour la sécurité intérieure a été publiée *au Journal officiel du* 19 mars 2003.

Ce texte traduit les lignes directrices de la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure qui nécessitaient, pour entrer en vigueur, l'adoption de dispositions d'ordre législatif.

Outre que la nouvelle loi prolonge de deux années, soit jusqu'au 31 décembre 2005, les mesures exceptionnelles instituées par la loi du 15 novembre 2001 sur la sécurité quotidienne afin d'agir plus efficacement contre le terrorisme, certaines de ses dispositions entrent directement dans le champ de compétence de la loi du 6 janvier 1978 « Informatique et libertés ».

Il en est ainsi de son article 21 qui donne un fondement législatif à l'existence des fichiers de la police judiciaire, en définit les contours et les caractéristiques ainsi que les destinataires en France, et de son article 24 qui définit les organismes étrangers ou internationaux qui peuvent être destinataires des informations nominatives traitées et enregistrées dans ces fichiers.

Relèvent aussi du champ d'application de la loi du 6 janvier 1978 l'article 23 de la loi qui a pour objet de compléter les motifs d'inscription dans le fichier des personnes recherchées et l'article 25 qui, en modifiant la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, élargit encore les cas dans lesquels les fichiers de police judiciaire peuvent être consultés à des fins non plus de police administrative, mais simplement administratives[1].

L'article 29 de la loi étend à nouveau, après la loi sur la sécurité quotidienne du 15 novembre 2001, la liste des infractions pouvant justifier le relevé d'une empreinte génétique et sa conservation dans le fichier national des empreintes génétiques créé par la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. Il prévoit également la

[1] On rappellera ici que c'est par le biais d'un amendement gouvernemental adopté lors des débats sur le projet de loi sur la sécurité quotidienne qui sont intervenus juste après les attentats du 11 septembre 2001, qu'a été autorisée la consultation des fichiers de travail de la police judiciaire à des fins de police administrative, et singulièrement à l'occasion d'enquêtes dites « de moralité ».

possibilité de conserver les empreintes des personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis l'une de ces infractions, ainsi que la possibilité d'enregistrer dans ce fichier les traces génétiques relevées à l'occasion des procédures de recherche des causes de la mort, de celles de recherche des causes d'une disparition et des empreintes génétiques correspondant ou susceptibles de correspondre à celles de personnes décédées ou recherchées.

Relève enfin du champ de compétence de la Commission l'article 30 de cette loi qui réprime le fait, pour les personnes soupçonnées d'avoir commis une des infractions pouvant donner lieu à inscription dans le fichier national des empreintes génétiques, de refuser de se prêter à un prélèvement.

La CNIL a estimé que ces dispositions posaient, sur trois points, des questions graves au regard des principes généraux de la protection des données personnelles.

A. La légalisation de l'existence des fichiers de police judiciaire

1. DES GARANTIES INSCRITES DANS LA LOI

La CNIL a noté en premier lieu que l'existence des fichiers de police judiciaire, à commencer par celui de la police nationale, le système de traitement des infractions constatées (STIC), dont les règles sont fixées par un décret du 5 juillet 2001, serait désormais consacrée par la loi, comme elle l'avait souhaité dans sa délibération du 19 décembre 2000 par laquelle elle avait émis un avis favorable assorti de réserves à la mise en œuvre, par le ministère de l'Intérieur, du STIC *(cf. 21*e rapport d'activité, p. 73 et ss.).

De même, le respect des principes dont la Commission est la gardienne ne peut que se trouver renforcé par l'inscription dans un texte législatif de certaines garanties jugées par elle indispensables s'agissant d'un fichier national recensant des informations nominatives issues de procédures pénales et non de condamnations prononcées de façon définitive. Il en est ainsi :
— du contrôle sur les traitements du procureur de la République territorialement compétent ;
— de la définition des personnes mises en cause ;
— du principe de limitation de la durée de conservation des informations traitées et enregistrées ;
— du renforcement du principe de la mise à jour, voire, dans certaines conditions, de l'effacement des données nominatives concernant aussi bien les personnes mises en cause que les victimes.

2. UN PAS VERS LA RÉGULARISATION DE JUDEX

C'est en décembre 2002 que parallèlement au débat sur le projet de sécurité intérieure, le ministère de la Défense a présenté à la CNIL un projet de création de son fichier d'enquêtes de police judiciaire dont la CNIL avait toutes les raisons de savoir qu'il fonctionnait depuis de nombreuses années.

La CNIL a salué cette démarche de régularisation et a saisi l'occasion, lors de l'examen en séance plénière le 9 janvier 2003, de rappeler toute l'importance qu'elle attache aux nécessaires garanties devant entourer la constitution, l'utilisation et la consultation des fichiers centralisés de procédures pénales ne mentionnant pas les suites judiciaires des affaires ayant donné lieu à inscription.

Ce traitement, mis en œuvre par le ministère de la Défense et similaire au STIC géré par le ministère de l'Intérieur, est constitué en effet de trois bases différentes : « JUDEX-AFFAIRES » et « JUDEX-PERSONNES MISES EN CAUSE », mises en œuvre au niveau national, et « JUDEX-GROUPEMENT », mise en œuvre de façon déconcentrée dans chaque département et recensant des informations sur les affaires et les personnes mises en cause, mais uniquement pour les faits commis dans le département concerné.

Le système d'information judiciaire JUDEX est mis à disposition de l'ensemble des officiers et des sous-officiers de gendarmerie et des gendarmes adjoints volontaires exerçant des missions de police judiciaire au sens de l'article 14 du Code de procédure pénale, chaque utilisateur devant faire l'objet d'une désignation par l'autorité hiérarchique.

Le système JUDEX étant de même nature que le STIC, le projet de décret qui a été soumis à la Commission reprenait les dispositions du décret du 5 juillet 2001 portant création du STIC, à l'exception de la prise en compte de quelques éléments nouveaux.

La Commission a constaté que les garanties qu'elle avait jugées nécessaires lors de l'examen du STIC et qui avaient été reprises par le ministère de l'Intérieur dans le décret portant création de ce fichier se retrouvaient dans le projet de décret portant création du système d'information judiciaire JUDEX.

Elle a néanmoins demandé, lors de son examen :
— que le signalement dans le fichier JUDEX ne soit possible qu'à partir d'un âge minimal, compatible avec les principes de notre droit pénal en matière d'enfance délinquante ;
— qu'une distinction soit faite entre personnels disposant d'un accès en temps réel aux bases du système JUDEX et les organismes pouvant se voir communiquer de façon ponctuelle des informations issues de ces bases ;
— que les pays dans lesquels sont implantés ces organismes disposent d'une législation de protection des données présentant des garanties équivalentes à celles du droit français.

Compte tenu du vote de la loi sur la sécurité intérieure, ce projet de décret n'a pas abouti et devra être repris dans le nouveau cadre législatif.

3. LA DÉCISION DU CONSEIL CONSTITUTIONNEL

Saisi de la loi pour la sécurité intérieure, le Conseil constitutionnel a considéré dans sa décision du 13 mars 2003 que l'ensemble des garanties que ce texte offre en matière de création et d'utilisation des fichiers de police *« est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ».*

Au-delà des garanties dont la Commission a déjà eu par le passé l'occasion de rappeler l'importance s'agissant des fichiers de police, le Conseil relève que :

— les destinataires de ces informations, autres que les magistrats de l'ordre judi ciaire, sont limitativement énumérés et doivent être habilités ;
— l'article 39 de la loi du 6 janvier 1978, modifié par le projet de loi, fixe les conditions de communication aux intéressés des informations traitées dans les fichiers de police judiciaire.

Le Conseil rappelle cependant, dans une réserve expresse (§ 43), que toutes les personnes inscrites dans ces fichiers doivent pouvoir exercer le droit d'accès et de rectification prévu par l'article 39 de la loi du 6 janvier 1978.

La CNIL a estimé que les fichiers de police judiciaire, comme tous les autres fichiers nominatifs, devaient respecter l'ensemble des conditions définies par la loi du 6 janvier 1978, notamment la consultation de la CNIL lors de la création de tout nouveau traitement de ce type, afin que soient précisément définies dans chaque cas la finalité du traitement, les catégories d'informations nominatives enregistrées, les infractions retenues, les modalités du droit d'accès, ainsi que les mesures prises en matière de sécurité du traitement.

La Commission aurait souhaité qu'une référence expresse à la loi du 6 janvier 1978 soit faite dans l'article du projet de loi institutionnalisant l'existence des fichiers de police judiciaire.

Si une mention explicite n'a pas été ajoutée, à l'initiative du gouvernement ou par amendement parlementaire, l'application complète de la loi de 1978 a fait l'objet d'engagements clairs du gouvernement et le Conseil constitutionnel rappelle dans une réserve expresse (§ 26) de sa décision du 13 mars 2003 que les dispositions de la loi du 6 janvier 1978, qu'il considère comme « protectrices de la liberté individuelle » depuis sa décision n° 97-389 du 22 avril 1997, s'appliqueront aux traitements dont la création est envisagée.

La Commission avait en outre estimé que la possibilité qui serait reconnue aux services de police et de gendarmerie d'enregistrer et de conserver, dans les fichiers de police judiciaire, des informations sur des personnes « sans limitation d'âge », posait le problème du signalement des enfants dans ces fichiers au regard des dispositions relatives à la responsabilité pénale des mineurs.

Sur ce point, le Conseil constitutionnel a jugé que le seul fait que cette disposition du projet de loi ne comporte pas de limitation d'âge ne méconnaît pas les principes dégagés en matière de responsabilité pénale des mineurs mais a demandé, dans une réserve expresse (§ 38), que le décret prévu à l'article 21 détermine la durée de conservation des informations enregistrées concernant des mineurs, celle-ci devant concilier la nécessité d'identifier les auteurs d'infractions et les principes applicables aux mineurs délinquants.

B. La consultation des fichiers de police judiciaire à des fins administratives

La loi sur la sécurité intérieure élargit la possibilité, déjà ouverte par la loi sur la sécurité quotidienne du 15 novembre 2001, de consulter les fichiers de police judiciaire pour les besoins de certaines missions de police administrative ou de sécurité comportant des risques d'atteinte à l'ordre public ou à la sécurité des personnes, à la

réalisation d'enquêtes et de tâches administratives, nombreuses, permanentes et pratiquées sur l'ensemble du territoire, telles que l'instruction des demandes d'acquisition de la nationalité française, des demandes de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers, ainsi que la nomination et la promotion dans les ordres nationaux.

La CNIL continue d'estimer que cette extension risque de faire jouer aux fichiers de police judiciaire le rôle d'un casier judiciaire parallèle, sans présenter les garanties ni les modalités de contrôle qui entourent aujourd'hui le casier judiciaire national automatisé, alors même que leur objet, leurs conditions d'accès, les modalités structurelles de leur alimentation et les délais inévitables de prise en compte de toute mesure d'effacement ou de mise à jour devraient cantonner ces fichiers à un rôle d'instruments de police judiciaire, sauf dans quelques cas bien précis et rigoureusement contrôlés.

Cet usage qui ne correspond pas à la finalité initiale (et réaffirmée par la loi) des fichiers d'enquêtes et de statistiques criminelles est d'autant plus problématique que ces nouvelles possibilités de consultation des fichiers de police à des fins administratives seraient ouvertes même si la procédure judiciaire concernée est toujours en cours, c'est-à-dire avant même d'être sûr que la personne mise en cause ne bénéficiera pas d'une décision de classement sans suite, comme il s'en produit plus de 300 000 par an, d'une mesure de non-lieu, voire sera acquittée ou relaxée.

Dans tous les cas, la Commission estime que l'élargissement des possibilités de consultation des procédures de police judiciaire à certaines enquêtes administratives de sécurité implique que soit menée une réflexion complémentaire sur le rôle que doit jouer le casier judiciaire national automatisé. Le ministre de l'Intérieur s'est dit favorable à une telle réflexion.

La Commission a donc réaffirmé que la consultation des fichiers de police judiciaire ne pouvait, à son sens, avoir lieu à des fins administratives que pour des « missions de police administrative ou de sécurité », seulement lorsque la nature de ces missions ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et selon des modalités rigoureuses s'agissant de l'habilitation des personnes pouvant y avoir accès, comme la Commission l'a déjà admis.

Sur ce point, le décret prévu en application de l'article 21 de la loi, qui sera pris après avis de la CNIL, précisera les conditions dans lesquelles les informations nominatives enregistrées dans les fichiers de travail de la police judiciaire pourront être consultées dans le cadre de « missions de police administrative ou de sécurité ».

La Commission estime qu'elle devrait également être consultée sur la teneur du décret fixant la liste des emplois et fonctions pour lesquels l'enquête administrative peut donner lieu à consultation des fichiers de police.

C. L'extension du fichier national automatisé des empreintes génétiques

La loi sur la sécurité intérieure modifie substantiellement le champ d'application du fichier national automatisé des empreintes génétiques (FNAEG) tant en ce qui concerne les infractions visées que les personnes pouvant faire l'objet d'un signalement dans ce fichier.

La loi étend ainsi le champ des infractions concernées, jusqu'alors limité aux infractions sexuelles et à certains crimes, à de nombreux délits de violence contre les personnes et d'atteinte aux biens ou mettant en danger l'ordre public, comme les délits en matière d'armes et d'explosifs.

Mais la principale modification concerne les critères d'inscription dans ce fichier. Peuvent désormais y figurer les personnes *« à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées à l'article 706-55* [du Code de procédure pénale] ». Les empreintes génétiques de ces personnes, simplement soupçonnées, pourront désormais être conservées dans le fichier alors que jusqu'à présent seules l'étaient les empreintes génétiques des personnes condamnées définitivement.

En outre les empreintes génétiques des personnes soupçonnées pourront être conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction.

Cette extension modifie profondément la nature même de ce fichier et implique en conséquence l'adoption de garanties nouvelles s'agissant tout particulièrement de ses modalités d'alimentation et des règles de conservation et d'effacement des informations nominatives traitées.

La Commission aurait souhaité que l'initiative de l'inscription dans ce fichier ne puisse relever que de la décision d'un magistrat et ne puisse résulter de celle d'un officier de police judiciaire, ce d'autant que le critère d'inscription des personnes suspectées — *« des indices graves ou concordants rendant vraisemblable [...] »* — laisse une très grande marge d'appréciation. Le même choix aurait dû s'imposer en ce qui concerne les décisions de rapprochement de l'empreinte génétique d'une personne suspectée avec les données incluses dans le fichier.

La Commission a noté toutefois que, conformément aux souhaits qu'elle avait exprimés lors des avis favorables rendus sur les modalités de fonctionnement du fichier des empreintes génétiques, les empreintes génétiques ne pourront être réalisées qu'à partir de segments d'ADN non codant, comme le précisent déjà les articles R. 53-9 et suivants du Code de procédure pénale.

Elle a pris également acte, au titre des garanties prévues, que le fichier national automatisé des empreintes génétiques, comme les fichiers de police judiciaire, demeure placé sous le contrôle d'un magistrat et que les empreintes conservées pourront être effacées sur instruction du procureur de la République agissant soit d'office, soit sur demande de l'intéressé, lorsque leur conservation n'apparaîtra plus nécessaire au regard de la finalité du fichier. Dans le cas où le procureur n'a pas ordonné

l'effacement, un double recours est prévu au bénéfice de l'intéressé auprès du juge des libertés et de la détention puis, en cas de contestation de la décision de ce dernier, auprès du président de la chambre de l'instruction.

La Commission a estimé cependant que des dispositions de suppression automatique des données devraient également être prévues lorsque la procédure est close et l'intéressé mis hors de cause, en particulier en cas de relaxe ou d'acquittement.

Enfin, et à l'instar des dispositions prévues pour les fichiers de police judiciaire, selon la Commission, la loi aurait dû également préciser les destinataires des informations issues du fichier des empreintes génétiques.

Un décret en Conseil d'État, pris après avis de la CNIL, déterminera notamment la durée de conservation des informations enregistrées qui devra être fixée en fonction de l'âge et de la gravité de l'infraction.

Sur les dispositions relatives au fichier national automatisé des empreintes génétiques, le Conseil constitutionnel a considéré, dans sa décision du 13 mars 2003, que les termes de la loi satisfont aux règles de la légalité constitutionnelle. Il relève toutefois qu'en cas de refus de prélèvement de la personne et en dehors des voies d'exécution d'office, le juge pénal devra proportionner la peine spécifique prévue par la loi à celle qui pourra être infligée pour le crime ou le délit qui aura justifié le prélèvement.

II. L'EXPLOSION DES DEMANDES DE DROIT D'ACCÈS AUX FICHIERS DE POLICE JUDICIAIRE ET DE GENDARMERIE

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

A. Données générales

Depuis sa création, la CNIL a reçu 7 523 demandes de droit d'accès indirect qui ont donné lieu à plus de 12 500 investigations et le nombre de ces requêtes augmente régulièrement d'une année sur l'autre. Comme on l'a déjà souligné dans le chapitre préliminaire, on peut même parler d'une véritable « explosion » du nombre des demandes. Pour la seule année 2002, la Commission a ainsi été saisie de 1 264 demandes (+ 51 % par rapporta 2001), qui ont donné ou vont donner lieu à plus de

2 500 vérifications, une même requête pouvant concerner plusieurs traitements (par exemple, le fichier des renseignements généraux, le N-SIS Schengen et les deux fichiers centralisés de police judiciaire — le STIC et JUDEX).

Évolution des demandes de droit d'accès indirect depuis 1995

	1995	1996	1997	1998	1999	2000	2001	2002
Requêtes	243	320	385	401	671	817	836	1 264
Évolution		**+** 32 **%**	**+** 20 **%**	**+ 4 %**	**+ 67 %**	**+** 22 **%**	**+ 2,4 %**	+ 51 %

Les requérants saisissent la CNIL :
— à la suite d'un refus d'embauche ;
— à la suite d'une enquête d'habilitation défavorable ;
— à l'occasion d'une candidature à un emploi du secteur public ;
— à la suite d'un refus de délivrance de visa ou de titre de séjour du fait de l'inscrip tion dans le système d'information Schengen ;
— à la suite d'une interpellation par les services de police ou de gendarmerie ;
— à la suite d'articles de presse sur les fichiers des renseignements généraux ou de police ou d'informations diffusées sur des sites internet décrivant les modalités de droit d'accès aux fichiers de police.

Au cours de l'année 2002, 2 315 vérifications ont été effectuées[1], dont 94 % opérées dans les fichiers du ministère de l'Intérieur.

Ministère de l'Intérieur	**2 184**
— Renseignements généraux (RG)	1 012
— Police judiciaire (PJ)	304
— Police urbaine (PU)	141
— Direction de la surveillance du territoire (DST)	66
— Système d'information Schengen (SIS)	661
— Direction de la sûreté et de la protection du secret.	—
Ministère de la Défense	**129**
— Gendarmerie nationale (GEND)	73
— Direction de la protection de la sécurité de la défense (DPSD)	32
— Direction générale de la sécurité extérieure (DGSE).	24
Ministère des Finances	**2**
— Fichier national informatisé de documentation de la direction générale des douanes et droits indirect (FNID)	**2**
— Fichier du traitement du renseignement et action contre les circuits Financiers clandestins.	**—**
Total	**2315**

[1] Ces 2 315 vérifications concernent des saisines reçues au cours des années 1999, 2000, 2001 et 2002 ; la recherche d'une éventuelle fiche peut prendre plusieurs mois et plusieurs investigations notamment pour le contrôle des suppressions.

B. Les fichiers de police judiciaire

Le résultat des investigations menées en 2002, à l'exclusion de celles relatives aux renseignements généraux (1 012) et du système d'information Schengen (661), soit 642 investigations menées est le suivant :

Fichiers	PJ	PU	DST	DSPS	GEND	DPSD	DGSE	FNID	TRACFIN	**Total**
Pas de fiche	129	95	55	—	26	24	24	2	—	**355**
Fiche sans suppression d'informations	111	39	11	—	40	7	—	—	—	**208**
Suppression totale ou partielle d'informations	40	3	—	—	6	1	—	—	—	**50**
Mise à jour de la fiche	24	4	—	—	1	—	—			29
Total	304	141	66	—	73	32	24	2	—	**642**

Les investigations menées dans les fichiers de police judiciaire et en particulier dans le système de traitement des infractions constatées (STIC) ont conduit la CNIL à faire procéder dans 37 % des cas (64 saisines sur les 175 requérants fichés à la police judiciaire) à des mises à jour ou même à la suppression de signalements erronés ou manifestement non justifiés.

Ainsi, un requérant s'est vu refuser un stage dans une juridiction parce qu'il était signalé dans le STIC comme « mis en cause » dans une affaire de vol de cyclomoteur alors même que, eu égard aux durées de conservation fixées par le décret du 5 juillet 2001 portant création de ce fichier, ces informations n'auraient plus dû figurer dans le traitement. Les commissaires de la CNIL en charge du droit d'accès indirect ont en conséquence demandé aux services de police judiciaire de supprimer la fiche correspondante ; ces derniers en ont avisé le procureur de la République de la juridiction concernée afin que la candidature du requérant soit réexaminée.

De même, un requérant était signalé dans le STIC à la suite de sa garde à vue, en tant que témoin, dans une enquête concernant une affaire de trafic de fausse monnaie datant de 1984. À la demande des magistrats de la CNIL, les services de police judiciaire ont procédé à la suppression de la fiche de l'intéressé.

Un autre requérant, qui avait déposé une plainte contre une banque, était signalé dans le STIC comme auteur d'une dénonciation calomnieuse à la suite de « l'interprétation » par un enquêteur de sa démarche. Sa fiche a donc été supprimée à l'occasion de l'exercice du droit d'accès indirect.

Il est particulièrement regrettable que la procédure de communication des fiches du STIC aux personnes concernées, avec l'accord du ministère de l'Intérieur et

du procureur de la République compétent, qui est prévue par le décret du 5 juillet 2001 créant le STIC, n'ait toujours pas pu être mise en œuvre.

C. Les fichiers des renseignements généraux

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

En pratique, trois situations peuvent se présenter :

1) Si les renseignements généraux ne détiennent aucune information nominative concernant un requérant, la CNIL en informe alors ce dernier, en accord avec le ministre de l'Intérieur.

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

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

Il faut souligner que ces règles propres aux fichiers des renseignements généraux viennent d'être étendues à l'ensemble des fichiers de sécurité publique par la loi de sécurité intérieure qui a modifié en ce sens l'article 39 de la loi du 6 janvier 1978.

Il convient de préciser que, pour les renseignements généraux, les recherches portent à la fois sur le fichier informatique d'indexation et sur le dossier individuel, sur les extraits de dossiers collectifs contenant des données nominatives sur les demandeurs, ainsi que sur les dossiers conservés dans les sections spécialisées de la direction centrale des renseignements généraux.

En outre, lorsqu'un document de synthèse citant des personnes physiques est établi par les services des renseignements généraux, une mention de ce document est faite dans le registre d'indexation des personnes physiques et si possible dans les dossiers individuels des personnes concernées.

Bilan des 1012 investigations menées en 2002 dans les fichiers des renseignements généraux

	Investigations aux fichiers des RG	% du total des vérifications effectuées aux RG
Requérants non fichés aux RG	776	77 %
Requérants fichés aux RG	236	23 %
Total	1 012	100 %

Sur 236 requérants fichés, les dossiers ont été communiqués dans les proportions suivantes

	Requérants fichés aux RG	% sur le nombre de requérants fichés
Dossiers jugés non communicables	**36**	15 %
Communication refusée par le ministre de l'Intérieur	**0**	
Communication acceptée par le ministre de l'Intérieur dont : — communication totale — communication partielle	**200** 199 1	85 %
Total	**236**	100 %

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 consultation des pièces communicables du dossier s'effectue au siège de la CNIL lorsque les requérants sont domiciliés dans la région Île-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 200 communications qui ont été effectuées en 2002 :
— 64 ont eu lieu au siège de la CNIL ;
— 136 ont été effectuées par l'autorité préfectorale du lieu de résidence de l'intéressé.

À la suite de ces communications, seuls quinze requérants ont rédigé une note d'observation qui a été insérée dans le dossier des renseignements généraux les concernant.

Par ailleurs il a été procédé à :
— la suppression totale de huit dossiers ;
— la suppression partielle de cinq dossiers.

Évolution des investigations aux renseignements généraux depuis le décret du 14 octobre 1991

Année	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	**2002**
Nombre de demandes traitées	766	320	273	197	252	352	282	270	365	576	**1 012**
Requérants non fichés aux RG	421	177	164	113	145	213	169	173	261	415	**776**
(% du total des vérifications]	55 %	*55 %*	60 %	57 %	58 %	60 %	60 %	64 %	71 %	72 %	**76 %**
Requérants fichés aux RG	345	143	109	84	107	139	113	97	104	161	**236**
(% du total des vérifications)	45 %	45 %	40 %	43 %	42 %	40 %	40 %	46 %	29 %	28 %	23 %
Dossiers jugés non communicables (%sur le nombre de requérants fichés)	90 26 %	50 35 %	44 40 %	25 30 %	33 31 %	*57* 41 %	23 20 %	15 15 %	18 17 %	35 22 %	**36** 15 %
Communication refusée par le ministre de l'Intérieur	13	0	0	0	0	0	0	0	0	0	0
(% sur le nombre requérants fichés)	4 %										
Communication acceptée par le ministre de l'Intérieur	242	93	65	59	74	82	90	82	86	126	**200**
(% sur le nombre de requérant fichés) dont :	70 %	65 %	60 %	70 %	69 %	59 %	80 %	85 %	83 %	78 %	85 %
— communication totale	200	*75*	27	44	63	*75*	84	79	85	126	**199**
— communication partielle	42	18	38	15	11	*7*	6	3	1	—	1

D. Les investigations au système d'information Schengen

Depuis l'entrée en vigueur du décret n° *95-577* du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS, aux termes de l'article 6 de ce décret et des articles 109 et 114 de la convention Schengen, la CNIL a reçu 1 855 (dont 661 au cours de l'année 2002) demandes de droit d'accès aux fichiers du système d'information Schengen.

Évolution du nombre de demandes de droit d'accès au N-SIS par année

Année	Nombre	Total cumulé
1995	22	22
1996	20	42
1997	21	63
1998	78	141
1999	359	500
2000	397	897
2001	297	1 194
2002	661	1 855

Parmi les 1 855 demandes de droit d'accès indirect au système d'information Schengen, 650 requérants étaient signalés.

Ces 650 signalements proviennent par ordre décroissant des pays suivants

Pays signalant	Nombre de signalements	Total cumulé
Allemagne	312	48,0 %
France	230	35,0 %
Italie	68	10,5 %
Espagne	21	3,5 %
Pays-Bas	5	1,0 %
Belgique	2	0,5 %
Grèce	10	1,0 %
Autriche	2	0,5 %
Total	650	100,0 %

Suite aux démarches entreprises par la CNIL, 273 signalements ont été supprimés du N-SIS (42 %), dont 215 par l'Allemagne, 40 par la France, 10 par l'Italie, 4 par l'Espagne, 3 par les Pays-Bas, 1 par la Belgique.

Dès lors, qu'aucun signalement n'est enregistré dans le système d'information Schengen, la CNIL poursuit ses investigations en saisissant le ministère des Affaires étrangères afin de connaître le motif du refus de visa et en particulier l'inscription éventuelle du requérant dans un fichier d'attention.

Ces fichiers gérés par le ministère des Affaires étrangères et en particulier par les postes consulaires sont désormais intégrés dans le nouveau système informatique de délivrance des visas (RMV2), créé par un arrêté du 22 août 2001 pris après avis favorable de la CNIL (délibération n° 01-019 du 15 mai 2001, *cf.* 22e rapport, p. 249).

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

A la demande de la CNIL, le ministère des Affaires étrangères s'est engagé à prendre toutes mesures de nature à faciliter l'exercice de ce droit et à permettre aux commissaires en charge du droit d'accès indirect de vérifier le contenu des fichiers d'attention.

III. DES PLAINTES CONTRE L'UTILISATION DES FICHIERS DE SÉCURITÉ PUBLIQUE

En dehors des demandes de droits d'accès indirect, la CNIL est régulièrement saisie par des particuliers qui s'interrogent ou s'inquiètent de l'utilisation faite de certains fichiers de sécurité, par les administrations. Dans de tels cas, la Commission vérifie que les règles de protection des données sont respectées et informe les plaignants de la réglementation en vigueur et du régime d'utilisation de tel ou tel fichier. À titre d'illustration de cette démarche, sont présentés deux cas réels mais anonymisés qui ont été traités en 2002 par la CNIL.

A. L'accès au casier judiciaire dans le cadre d'une enquête de moralité

M. X. se voit refuser, par la préfecture de police de Paris, un certificat provisoire d'aptitude à la conduite de voitures de grande remise (habilitation à être chauffeur de personnalités), au motif que son casier judiciaire mentionnait qu'il avait fait l'objet d'une condamnation d'un mois d'emprisonnement avec sursis pour rébellion par jugement du tribunal correctionnel de Paris. Ce refus lui est notifié par courrier.

M. X. est très étonné des termes de ce courrier dans la mesure où, lors du dépôt de sa demande, la préfecture lui avait demandé un extrait de son casier judiciaire (bulletin n° 3) qui était vierge (mention : « néant »). Il saisit la CNIL pour obtenir des éclaircissements.

Lors de l'instruction des demandes de certificats d'aptitude à la conduite de voitures de grande remise, le préfet vérifie, notamment, les conditions de moralité du demandeur, conformément aux dispositions du décret 55-961 du 15 juillet 1955. À cette fin, la préfecture de police de Paris peut obtenir communication, auprès des services du casier judiciaire, du bulletin n° 2 du casier judiciaire des demandeurs.

À la différence du bulletin n° 3 du casier judiciaire qui ne fait état, pour l'essentiel, que des condamnations à une peine d'emprisonnement ferme supérieure à deux ans, le bulletin n° 2 mentionne beaucoup plus de condamnations, même moins graves. Il n'est remis qu'à certaines autorités administratives. L'article R. 79-3° du Code de procédure pénale prévoit, notamment, que le bulletin n° 2 du casier judiciaire est délivré aux administrations *« chargées de l'assainissement des professions agricoles, commerciales, industrielles ou artisanales »*.

Ainsi, la mention de cette condamnation dans le bulletin n° 2 du casier judiciaire de M. X., dont fait état la préfecture de police de Paris à l'appui de son refus de délivrance d'un certificat provisoire d'aptitude à la conduite de voitures de grande remise, n'a appelé aucune observation particulière au regard des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

B. L'accès au fichier des immatriculations en cas de stationnement illicite

M.G. a garé son véhicule — en stationnement gênant, vraisemblablement — sur le parking d'une co-propriété. Quelques jours plus tard, il reçoit du syndic de copropriété un courrier lui demandant d'enlever son véhicule de ce stationnement et de ne plus y stationner à l'avenir.

M. G. s'interroge sur les méthodes utilisées par cet organisme pour obtenir son identité et son adresse.

La procédure qui est suivie dans ces cas est prévue par les articles R. 325-47 à R. 325-52 du Code de la route. Ces articles précisent que, dans le cas où un véhicule est laissé sans droit dans des lieux non ouverts à la circulation publique, ce qui est le cas du parking d'un immeuble privé, le maître des lieux qui veut faire procéder à l'enlèvement de ce véhicule adresse sa demande à l'officier de police territorialement compétent.

L'article R. 325-49 du Code de la route ajoute que lorsque le maître des lieux ne connaît pas l'identité et l'adresse du propriétaire du véhicule, l'officier de police judiciaire lui communique celles-ci, afin de lui permettre d'adresser une mise en demeure au propriétaire du véhicule lui demandant de retirer son véhicule dans les huit jours. Dans le cas où cette mise en demeure est infructueuse, le maître des lieux saisit à nouveau l'officier de police judiciaire qui prescrit la mise en fourrière du véhicule.

La CNIL a apporté ces précisions à plusieurs plaignants qui l'ont interrogée dans des cas similaires.

IV. LA DIMENSION EUROPEENNE ET INTERNATIONALE

En France, l'impact des événements terroristes du 11 septembre 2001 sur la protection des données personnelles a été relativement modéré[1] au regard de ce qui s'est passé chez nos voisins et outre-Atlantique. Cette relative modération trouve son explication dans le fait que la France est dotée, depuis 1986, d'une législation anti-terroriste qui a été adoptée à la suite d'une vague d'attentats criminels. Cette législation prévoit notamment une centralisation des poursuites pénales en matière de crimes et délits terroristes, des juridictions spécialisées pour juger des crimes terroristes et des pouvoirs de police judiciaire plus étendus dans ce domaine que dans d'autres hypothèses. Cette législation, validée par le Conseil constitutionnel en son temps, n'est plus contestée. De même, la France dispose, depuis 1988, d'une législation sur la fraude informatique qui est applicable en matière de virus informatique et, depuis 1991, d'une législation spécifique sur les interceptions de communications qui est applicable aux échanges sur internet. C'est plus le souci de la montée de la délinquance que la crainte du terrorisme qui a conduit en France à la fin de 2001 et en 2002 (cf. I du présent chapitre) à des modifications substantielles de son arsenal législatif.

C'est cette conclusion qu'a présentée la CNIL lors de la 24e conférence internationale des commissaires à la protection des données qui s'est tenue à Cardiff du 9 au 11 septembre 2002[2] au cours d'une session réservée à ce sujet.

Depuis les événements du 11 septembre 2001, l'ensemble des commissaires en charge de la protection des données en Europe et dans le monde suit avec attention ces questions. Dans ce contexte, ils estiment particulièrement importante leur mission d'exprimer librement et publiquement leurs avis pour éclairer leur gouvernement et l'opinion.

Dans ce contexte, deux séries d'initiatives européennes et internationales méritent d'être signalées. Celles de la conférence internationale de Cardiff et celle du groupe dit « de l'article 29 » à propos des exigences américaines relatives aux transferts, par les compagnies aériennes, des données qu'elles détiennent sur leurs passagers aux douanes américaines.

[1] 22e rapport annuel pour 2001, p. 17 sur la loi sur la sécurité au quotidien et notamment, page 21 sur l'obligation faite aux opérateurs de télécommunication et aux intermédiaires techniques de l'internet de conserver les données de connexion à des fins de police pour laquelle le décret d'application n'a pas encore été adopté.

[2] La conférence était organisée conjointement par les commissaires en charge de la protection des données en Irlande, à Jersey, Guernesey, et l'Ile de Man ainsi qu'au Royaume-Uni.

A. La conservation des données de connexion à des fins policières

Les autorités de protection de l'Union européenne ont fait part, dans une déclaration rendue publique, de leur inquiétude concernant les propositions examinées au sein du Conseil de l'Union européenne qui auraient pour conséquence la conservation systématique et obligatoire des données de trafic relatives à l'usage de tout moyen de télécommunication (ex. : détails concernant la durée et le lieu des appels, les numéros utilisés pour téléphoner, envoyer un fax, un e-mail et les données relatives aux usages d'internet) pour une durée d'un an ou plus, afin d'en permettre l'accès aux autorités chargées de vérifier l'application effective de la loi. Elles ont également exprimé leurs doutes quant à la légitimité et la légalité de telles mesures tout en attirant l'attention sur leur coût excessif pour l'industrie des télécommunications et de l'internet, ainsi que sur l'absence, apparemment paradoxale, de semblables dispositions dans le pays qui a été le plus concerné par des activités terroristes, les États-Unis.

Dans ce contexte, elles ont souligné une nouvelle fois qu'une telle mesure constituerait une atteinte aux droits fondamentaux garantis aux personnes par l'article 8 de la Convention européenne des Droits de l'homme, tel que précisé par la Cour européenne des Droits de l'homme. Ainsi elles ont indiqué que lorsque des données de trafic doivent être conservées, la nécessité d'une telle conservation doit être démontrée, la période doit être aussi courte que possible et cette pratique clairement établie par la loi, de façon à prévenir tout accès illégal ou toute autre forme d'abus. Ils ont enfin précisé en conclusion que la conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable.

De manière plus générale les représentants de plus de cinquante autorités de protection des données et des commissaires à la protection de la vie privée, cette fois-ci du monde entier participant à la conférence, ont dans un communiqué de presse résumé ainsi leurs conclusions : « *Alors qu'il est nécessaire de protéger la société des crimes tels que le terrorisme, la réaction de nombreux pays a été hors de proportion, et a eu de sérieuses implications sur la protection de la vie privée. Les commissaires estiment que la nécessité de protéger la vie privée à l'occasion de tels événements demeure une fâche essentielle pour la communauté internationale de protection des données. À moins que les gouvernements n'adoptent une approche qui prenne en compte les problèmes de protection des données personnelles à leur juste mesure, il est à craindre que ces gouvernements ne commencent à ébranler les plus fondamentales libertés, celles mêmes qu'ils cherchent à protéger.* »

B. Les exigences américaines en matière de transferts de données par les compagnies aériennes sur leurs passagers

Dans le cadre de la lutte contre le terrorisme et les actes criminels, les Etats-Unis ont adopté le 19 novembre 2001 une législation sur la sécurité de l'avia-

tion et du transport *(The Aviation and Transportation Security Act)* qui prévoit la communication aux services des douanes et de sécurité américains des informations personnelles traitées par les compagnies aériennes. La réglementation d'application de ces législations a prévu à cette fin l'accès direct par les douanes américaines aux bases de données tenues par les fournisseurs de services de réservations aériennes tels qu'Amadeus qui concerne essentiellement les compagnies européennes, Sabre et Galileo qui concernent essentiellement les compagnies américaines.

Créées de longue date par les compagnies aériennes, ces centrales d'informations, alimentées par les agences de voyages et les compagnies aériennes, constituent le seul instrument d'échange entre elles des informations nécessaires depuis le moment de la réservation jusqu'à la réalisation complète des prestations demandées au fur et à mesure par les passagers.

Ainsi les systèmes de réservations, qui dialoguent entre eux dans les cas où une réservation comporte un ou plusieurs vols sur des compagnies aériennes liées à des systèmes de réservations différents, portent sur des enregistrements d'informations standardisés au plan international dénommés « PNR » *(Passenger Name Record)* comprenant, pour partie selon les prestations offertes par les compagnies et demandées par leurs clients, les informations sur l'agence auprès de laquelle la réservation est effectuée, l'itinéraire complet du déplacement qui peut comporter plusieurs étapes, les indications des vols concernés (numéro des vols successifs, date, heures, classe économique, business, etc.), le groupe de personnes pour lesquelles une même réservation est faite, le contact à terre du passager (numéro de téléphone au domicile, professionnel etc.), les tarifs accordés, l'état du paiement effectué et ses modalités par carte bancaire, les réservations d'hôtels ou de voitures à l'arrivée.

Ces enregistrements concernent également les services à bord liés aux préférences alimentaires des passagers qui peuvent être à caractère religieux (les repas, végétarien, asiatique, cascher etc.), et les services liés à la santé (diabétique, aveugle, sourd, voiture roulante, assistance médicale, etc.).

Les compagnies aériennes qui ne donneraient pas satisfaction sont menacées par les autorités américaines de contrôles renforcés de leurs passagers et, ultérieurement, de se voir infliger des amendes ou retirer leurs droits d'atterrissage.

Le groupe dit de « l'article 29 » s'est saisi dès le mois d'octobre 2002 de la question en vue de contribuer de manière immédiatement commune à la résolution de ce problème. Dans son avis rendu le 24 octobre 2002 (cf. annexe 7 Groupe article 29) il fait état des nombreuses difficultés soulevées par cette affaire au regard du respect des droits des personnes assurés en Europe, notamment par la directive du 24 octobre 1995 (95/46).

Tout en reconnaissant la souveraineté des Etats-Unis à l'occasion du contrôle aux frontières, le groupe souligne en particulier les aspects suivants :

— le fait que là question de la lutte contre le terrorisme relève de la coopération judi ciaire et policière entre États ;

— le caractère excessif et disproportionné des données collectées au regard de la finalité poursuivie, notamment en ce qui concerne des données « sensibles » ;

— le non-respect du principe de finalité qui impose que les données ne soient pas traitées pour une autre finalité que celle indiquée au moment de la collecte ;
— la nécessité d'organiser la sécurité des données, pour interdire en l'espèce l'accès de tiers non autorisé ;
— la question du transfert des données dans un pays tiers vis-à-vis de laquelle la directive 95/46/Œ sur la protection des données impose de s'assurer que le pays destinataire garantit un niveau adéquat de protection des données, ce qui n'est pas le cas des États-Unis en la matière (le *Privacy Act* de 1974 applicable aux administra tions fédérales exclut explicitement les étrangers du bénéfice du régime de protection qu'il institue) ;
— la nécessité de procéder à l'information des passagers sur un tel transfert.

Le groupe a également souligné qu'un accès aux données des personnes ne voyageant pas à destination des États-Unis n'était pas pertinent. De même a-t-il souligné les difficultés majeures liées au transfert envisagé de données sensibles et biométriques à l'avenir, prévu par les autorités américaines pour l'année 2004.

Au plan national, la CNIL a attiré l'attention du Premier ministre par lettre en date du 12 décembre 2003 sur le caractère disproportionné et réellement excessif des transmissions d'informations exigées par les États-Unis et exprimé le souriait que le Gouvernement français prenne avec ses partenaires européens et avec la Commission européenne l'initiative d'une négociation.

De fait, la Commission européenne a entrepris des discussions avec les autorités américaines. Ces discussions menées avec les services des douanes américaines se sont poursuivies en début d'année 2003 en vue de parvenir à un accord.

Les États membres, la Commission européenne et le groupe dit de l'article 29 ont déployé des efforts diplomatiques pour faire repousser par deux fois la date limite fixée par les autorités américaines en vue de négocier un accord acceptable. Certaines garanties offertes par la partie américaine ont été reconnues par la Commission européenne dans le cadre d'une déclaration commune avec les douanes américaines en date du 18 février. En particulier les données relatives aux passagers dont les réservations ne donnent pas lieu à un débarquement, embarquement ou transit sur le sol des États-Unis, ne seraient pas utilisées par les autorités américaines.

Les grandes compagnies aériennes opérant sur le sol européen à destination des États-Unis ont dans ce contexte donné accès le 5 mars 2003 aux douanes américaines aux données relatives à leurs passagers qui sont contenues dans les systèmes de réservation tout en les en informant.

À l'heure de la rédaction du présent rapport, l'ensemble des questions soulevées par cette affaire par les commissaires européens en charge de la protection des données ne sont pas encore résolues ainsi que l'a souligné le Parlement européen dans une résolution du 12 mars 2003 très critique vis-à-vis de la Commission européenne.

C. Le rapprochement entre Europol et les États-Unis

Au lendemain des attentats terroristes du 11 septembre 2001, les relations entretenues par Europol avec les Etats-Unis, « pays tiers » au sens de la Convention du 26 juillet 1995, ont sans aucun doute pris une nouvelle dimension.

1. LA PROCEDURE D'ACCORD AVEC LES PAYS TIERS

On rappellera qu'aux termes de la Convention, Europol est invite à entretenir des relations avec des instances et États tiers — c'est-à-dire avec des États qui ne sont pas membres de l'Union européenne — dès lors que cela est utile pour l'accomplissement de ses missions. La Convention prévoit expressément la possibilité pour Europol de recevoir ou de transmettre des données à des États ou instances tiers sous certaines conditions. Ainsi, l'article 18 de la Convention dispose que la transmission d'informations doit être nécessaire pour la prévention ou la lutte contre les infractions relevant de la compétence d'Europol — au nombre desquelles figure le terrorisme international —, être admissible au regard des règles adoptées par le Conseil de l'Union européenne, et qu'un niveau adéquat de protection des données doit être garanti par l'État ou l'instance tiers.

En application de ces dispositions, le Conseil de l'Union européenne a adopté à l'unanimité différents actes précisant les règles relatives à la réception ou à la transmission de données : deux actes du 3 novembre 1998, l'un relatif à la réception d'informations émanant de tiers, l'autre à la transmission d'informations à des tiers, et l'acte du 12 mars 1999 arrêtant les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers. C'est ce dernier texte qui subordonne la transmission de données à caractère personnel à la conclusion d'un accord entre Europol et un État ou organe tiers.

Cette procédure a été suivie par Europol avec notamment la Pologne, la Hongrie, la République slovaque, la République tchèque, l'Estonie, la Suisse et Interpol. L'autorité de contrôle commune Europol (ACC) est appelée à se prononcer deux fois au cours de la procédure de négociations. Elle examine d'abord s'il existe ou non des obstacles empêchant Europol d'engager des négociations. Ceci nécessite pour l'ACC d'apprécier le niveau de protection des données offert par le futur partenaire d'Europol en tenant compte du type de données concernées, de leur finalité, de la durée du traitement envisagé, des spécificités éventuelles du pays ou de l'instance tiers concerné, de l'existence ou non d'un contrôle par une autorité indépendante. En second lieu elle se prononce sur le projet d'accord. C'est pourquoi elle a décidé d'élaborer des modèles standards d'avis qui traitent de manière systématique différentes questions relevant de la protection des données. Il en fut différemment avec les États-Unis.

2. LA SPÉCIFICITÉ DES RELATIONS AVEC LES ETATS-UNIS

La Convention Europol prévoit la possibilité, à titre exceptionnel, de transmettre des données personnelles à un État ou une instance tiers sur le seul fondement d'une décision du directeur d'Europol, dès lors qu'il considère que cette transmission

est absolument nécessaire pour sauvegarder les intérêts essentiels des États membres dans le cadre des objectifs d'Europol ou dans le but de prévenir un danger immédiat.

Cette procédure d'urgence a été suivie par le directeur d'Europol, M. Jurgen Storbeck, lorsqu'il a pris sa décision en date du 28 septembre 2001 concernant la transmission de données à caractère personnel aux services répressifs des États-Unis d'Amérique, et a répondu ainsi à la profonde émotion et à l'élan de solidarité engendrés par les événements du 11 septembre 2001, ainsi qu'à la demande du Conseil des ministres « Justice et affaires intérieures » (JAI) de l'Union européenne du 20 septembre 2001 consistant à prendre toutes les mesures nécessaires pour renforcer la coopération avec les États-Unis. Cette décision s'est révélée utile puisqu'elle a permis à l'Office européen de police de transmettre aux États-Unis des informations concernant certaines des personnes impliquées dans les attentats.

Sans contester la nécessité d'aider autant que possible les États-Unis dans la lutte contre le terrorisme, l'ACC s'est toutefois toujours montrée soucieuse de voir les principes de protection des données respectés. Elle a très rapidement fait part au directeur d'Europol de son souhait que la transmission d'informations personnelles aux autorités américaines repose sur un accord, seul fondement juridique susceptible de garantir le respect des droits des personnes. En conséquence, après avoir rappelé les principes essentiels de protection des données et demandé, en l'absence de rapport relatif au niveau de protection des données aux États-Unis, à être associée très étroitement aux négociations entre Europol et les autorités américaines (cette demande sera suivie d'effets puisque des représentants de l'ACC seront régulièrement associés aux réunions entre Europol et les autorités américaines), l'ACC a estimé dans son avis du 26 novembre 2001 que lesdites négociations pouvaient être engagées.

Parallèlement, l'ACC a tenu à faire connaître au directeur d'Europol ses observations sur sa décision du 28 septembre 2001, en particulier sur le caractère temporaire qu'elle devait revêtir et la nécessité de procéder périodiquement au réexamen de son bien-fondé *[cf.* avis du 6 mars 2002). Les négociations entre Europol et les États-Unis n'ayant pas encore conduit à un accord, une nouvelle décision a été d'ailleurs adoptée par le directeur le 1er juillet 2002.

L'accord entre Europol et les États-Unis — complété par un échange de lettres — a finalement été signé le 20 décembre 2002 à Copenhague. Ce texte, qui n'est pas parfait, est vraisemblablement le seul sur lequel les parties étaient susceptibles de s'entendre, tant leur approche de la protection des données est différente, notamment sur la nécessité — ou non — de mettre en place une autorité de contrôle indépendante ayant une compétence générale en la matière.

Or, il ne faisait aucun doute que, pour des raisons purement politiques — qui peuvent être comprises, dans les circonstances de l'époque — Europol mettrait tout en œuvre pour coopérer de manière étroite avec les États-Unis. Du côté américain, il avait été régulièrement rappelé que si un accord devait être conclu, il s'agirait alors d'une concession accordée dans le cadre d'Europol, mais que, en tout état de cause, les négociations pouvaient être interrompues à tout moment.

C'est pourquoi, l'ACC a tenu à souligner, dans son avis du 3 octobre 2002 l'effort produit dans le texte pour établir un juste équilibre entre la nécessité à la fois de lutter contre la criminalité grave et de préserver les droits des personnes. L'ACC n'a toutefois pas recouru à la rédaction habituelle, selon laquelle *« il n'existe pas d'obstacle à ce que le directeur conclue l'accord »,* et a seulement indiqué que le Conseil était à présent en mesure d'autoriser le directeur d'Europol à conclure l'accord. Cette « retenue » rédactionnelle traduit sans doute l'appréciation que porte l'ACC sur le texte, qui comporte des points positifs mais aussi des lacunes.

C'est ainsi que l'article 5 du texte fait état du principe de finalité. Il est en outre précisé que les informations transmises par Europol ne doivent être utilisées que par les autorités américaines compétentes, dans les conditions de l'accord (article 7), et que des données sensibles ne doivent être transmises que si cela est strictement nécessaire pour atteindre l'objectif poursuivi (article 6).

De plus, le projet dispose, conformément à l'article 18.4 de la Convention, que la transmission des données à des organismes internationaux ou des États tiers ne peut avoir lieu sans l'accord préalable de la partie qui les a communiquées, sauf si les informations sont déjà dans le domaine public.

D'autres aspects du projet suscitent, en revanche, plus d'inquiétude.

Il en est ainsi de la question de la durée de conservation des données. Si l'article 9.3 de l'accord prévoit que, dans l'hypothèse où l'une des parties est informée de ce que les données qui lui ont été transmises ne sont pas exactes, elle doit prendre toute mesure afin d'éviter que les services compétents utilisent ces données erronées, ce qui peut conduire à les compléter, les corriger ou les supprimer, cette disposition n'apporte aucune garantie générale relative à la durée de conservationdes données par les autorités américaines.

De même, la question du contrôle par une autorité indépendante du traitement des données, qui a fait l'objet de longues discussions lors des négociations, n'est que partiellement traitée.

L'article 12 de l'accord renvoie, pour la mise en œuvre effective du texte, aux organes de contrôle, judiciaires ou administratifs de chacune des parties, qui assureront un « niveau d'indépendance approprié ». Cet article doit être lu à la lumière de l'article 13, qui prévoit, à la demande expresse des représentants de l'ACC, une « consultation » (le terme *« d'évaluation »* n'ayant pas été accepté) de nature à permettre un contrôle effectif de l'application de l'accord par les Etats-Unis.

Les représentants américains ont indiqué qu'il existe différents organes, tant au niveau fédéral que des États, qui, bien que n'étant pas séparés du pouvoir administratif, sont en mesure d'effectuer un contrôle indépendant. En outre, un contrôle juridictionnel pourrait être opéré. Toutefois, les autorités américaines étant peu familiarisées avec un contrôle, même interne, en cette matière, il est essentiel que l'application de l'accord fasse l'objet d'un suivi, ce d'autant que des divergences d'interprétation de notions juridiques sont apparues lors des négociations.

Aussi, l'ACC estime que la procédure d'évaluation conjointe de la mise en œuvre de l'accord, prévue par l'article 14, qui doit être engagée dans un délai de

deux ans et à laquelle l'autorité devrait participer, est essentielle et permettra de vérifier si certains aspects du texte doivent être améliorés.

En tout état de cause, l'ACC s'est attachée dans son avis à souligner le caractère exceptionnel de la situation à laquelle les Etats-Unis doivent faire face, de manière à ce que l'accord conclu ne puisse constituer un précédent auquel il pourrait être fait référence lors de l'élaboration de projets d'accord avec d'autres pays tiers.

Chapitre 2

PROSPECTION COMMERCIALE : NOUVEAUX USAGES, NOUVEAUX REGARDS, NOUVELLES ACTIONS

Qu'est-ce qu'un « spam » ?

« Spam » :

— marque de *« corned-beef »,* acronyme de *Spiced Ham* (jambon épicé) :
— « Spam, spam, spam, spam, spam » extrait de la chanson des « Vikings » ama teurs de « spam » (Monty Python Flying Circus) ;
— courrier électronique non sollicité ;
— synonymes : courrier-rebut, pourriel, polluriel.

Mais il n'y a pas que le « spam ». D'autres problématiques apparaissent : marketing viral, base centralisée au niveau d'un groupe...

I. LA « BOITE A SPAMS »

Le 10 juillet 2002, la CNIL a ouvert une boîte aux lettres électronique (spam@cnil.fr) permettant aux internautes d'y transférer les messages électroniques non sollicités, appelés « spams », qu'ils reçoivent. Cette opération ponctuelle, achevée en novembre 2002 avec la fermeture de la « boîte à spams », s'inscrit dans la continuité du rapport *Publipostage électronique* adopté par la Commission en 1999[1] et atteste de sa volonté d'appréhender le phénomène du *« spamming »* et d'apporter aux internautes qui en sont victimes des éléments leur permettant d'y faire face.

[1] Délibération n° 99-048 du 14 octobre 1999 portant adoption du rapport relatif au publipostage électronique et la protection des données personnelles.

A. Un constat : l'ampleur du *« spamming »* en France

En l'espace de trois mois, environ 325 000[1] « spams » ont été reçus ce qui démontre la mobilisation qu'a suscitée l'opération « boîte à spams », les internautes trouvant enfin un relais institutionnel au problème du *« spamming »* face auquel ils sont, le plus souvent, désarmés, tant d'un point de vue technique que juridique. Il importe cependant de préciser que l'ensemble des messages reçus ne peut être considéré comme de réels « spams ».

En effet, le « spamming » est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. Constituent des « spams » les messages adressés sur la base d'une collecte irrégulière de mails, soit au moyen de moteurs de recherche dans les espaces publics de l'internet (sites web, forums de discussion, listes de diffusion, chat...), soit que les adresses aient été cédées sans que les personnes en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir. Une telle collecte est alors déloyale et illicite au sens de l'article 25 de la loi du 6 janvier 1978. En outre, ces messages n'ont pas, le plus souvent, d'adresse valide d'expédition ou de « répondre à » *(reply to)* et l'adresse de désinscription est inexistante ou invalide.

L'ensemble des messages reçus dans la « boîte à spams », et jugés par l'internaute émetteur être des « spams », ne répond pas à cette définition. Ainsi, certains internautes ont considéré comme étant du « spam » l'envoi, par exemple, par une de leurs connaissances d'un mél humoristique ou encore d'un message expédié à un destinataire autre. De la même façon, d'autres internautes ont assimilé à de la prospection électronique non sollicitée une lettre d'information *(newslefterj* envoyée à partir d'un site sur lequel ils s'étaient préalablement inscrits mais dont ils avaient oublié l'existence (c'est le cas, par exemple, d'un internaute se plaignant de la réception de la lettre d'information du journal *Le Monde* ou du Sénat). Certains internautes ont aussi interprété une opération de prospection électronique régulière comme étant du « spam » et ont transféré les messages ainsi reçus à l'adresse mise en place par la Commission. En l'état actuel du droit et au regard de la loi du 6 janvier 1978, une opération de prospection électronique est légale à la condition de satisfaire aux conditions classiques s'appliquant en la matière : loyauté de la collecte de l'adresse mél, déclaration du fichier servant de base à l'opération et possibilité, pour la personne démarchée, d'exercer son droit d'opposition à la cession des données.

Les cas mentionnés ci-dessus demeurent cependant marginaux et l'immense majorité des messages reçus mérite bien le qualificatif de « spam ». Le premier travail effectué à partir des messages reçus a été d'analyser leur contenu afin de permettre une classification et donc une meilleure compréhension du phénomène du *« spamming »* en France.

[1] Ce chiffre est une estimation basse, les internautes joignant parfois à leur message une pièce jointe qui comprend plusieurs « spams ».

B. Le « spam » : souvent un message pornographique ou de rencontres émanant d'une petite entreprise et « *made in USA* »

L'idée de proposer aux internautes français de transmettre les messages qu'ils considéraient être du « spam » répondait, entre autres objectifs, à celui de prendre la pleine mesure du phénomène du « *spamming »,* tant de manière quantitative que qualitative. Afin de nourrir le débat sur cette pratique, il importait de disposer de chiffres et de données fiables. Il faut souligner que c'est la première fois que des chiffres concernant le *« spamming »* en France émanent d'une autorité publique. Les méls reçus ont donc été classés, dans un premier temps, selon leur origine géographique supposée ce qui a permis d'établir que 84,8 % des « spams » étaient rédigés en langue anglaise, 8 % étaient d'origine asiatique tandis que 7 % étaient rédigés en langue française, la proportion de messages d'une langue autre (allemand, espagnol, etc.) étant négligeable.

Chaque catégorie — à l'exception des « spams » asiatiques — a ensuite fait l'objet d'une classification interne suivant le contenu du message et donc du destinataire visé. Ce choix a été effectué afin de déterminer quels types d'internautes était réellement visé puisque, par définition, une opération de « *spamming »* ne procède pas à un envoi ciblé. Il apparaît ainsi que ce sont les particuliers qui sont le plus visés par les contenus des « spams » puisque 85 % des « spams » proposent des produits ou des services susceptibles de les intéresser tandis que 15 % des « spams » sont orientés vers les besoins d'entreprises.

Les « spams » rédigés en langue anglaise ont été classés selon les thématiques suivantes indiquées par ordre croissant : assistance juridique (avocat, procédure civile, etc.), *avec* 0,2 % des messages reçus, jeux/casinos (1 %), tourisme (1,4 %), santé (Viagra, produits pour régimes, hormones, etc. : 12,9 %), produits financiers (crédits, remboursement de dettes, prêts, placements divers, etc. : 40 %), et enfin, les messages à caractère pornographique/rencontres représentent la thématique la plus importante (42 %).

Une classification plus précise a été appliquée aux « spams » de langue française. Afin de pouvoir en tirer de plus amples renseignements, les messages ont été scindés en deux grandes catégories en fonction du public ciblé, d'une part les messages visant à démarcher les particuliers et d'autre part les messages offrant des services aux entreprises.

S'agissant des « spams » visant les particuliers (démarchage commercial, incitation à consulter un site, proposition de services variés, etc.), il a été possible d'identifier certains domaines d'activité qui regroupent un nombre important d'entreprises émettrices de « spams ».

Les principaux secteurs à la source d'importantes opérations de prospection sont les suivants : crédits/finances/assurances avec 5 % des « spams » reçus, jeux/casinos (6,2 %), tourisme (6,5 %) et les offres de biens et de services en ligne (achats en ligne de biens de grande consommation et de services liés à internet) qui constituent 12,3 % des « spams » recueillis. Enfin, il faut souligner que les « spams »

à caractère pornographique ou de rencontres arrivent largement en tête puisqu'ils sont à l'origine de *55 %* des « spams » reçus.

D'autres secteurs ont pu être identifiés, mais ils ne représentent qu'une faible part des messages, il s'agit du secteur de la santé (0,5 % des « spams » reçus), de l'immobilier (0,9 %), de l'emploi (1,1 %), de la voyance (2,3 %) et du divertissement (2,3 %). Par ailleurs, une catégorie « escroquerie/chaînes/divers », correspondant à 3 % des « spams » français, a été créée afin de classer les messages atypiques ou proposant des offres douteuses.

S'agissant des messages offrant des services aux entreprises, les deux principaux secteurs identifiés sont le secteur « formation/emploi/recrutement » avec 5 % des « spams » reçus et surtout, le secteur des produits et services liés aux technologies de l'information et de la communication, dans lequel on retrouve les offres relatives aux aspirateurs de « méls*/ mailing list* », représentant 74 % des « spams » de cette catégorie.

En fin de compte, cette opération a permis, en premier lieu, de constater que la grande majorité des « spams » était anglophone, ce qui peut s'expliquer par le fait que près de 80 % du contenu présent sur internet est de langue anglaise et que l'utilisation d'internet est plus répandue aux Etats-Unis que partout ailleurs. Concernant le contenu des messages, l'analyse des objets des messages reçus permet de pointer des différences notables entre ceux reçus en langue française et ceux reçus en langue anglaise.

D'une part, dans le cas des « spams » d'origine anglophone, on peut remarquer la présence importante de « spams » dans les secteurs financiers et de la santé, respectivement 39,4 *%* et 12,9 *%.* Cette proportion ne se retrouve pas au sein des « spams » français et peut s'expliquer par un encadrement législatif et réglementaire bien plus strict de ces secteurs en France et dans l'Union européenne qu'aux Etats-Unis ainsi que par des habitudes de consommation des ménages sensiblement différentes des deux côtés de l'Atlantique. Toutefois, la proportion de « spams » à caractère pornographique est, sans surprise, la plus importante et elle est sensiblement la même que les messages soient rédigés en langue anglaise ou française.

D'autre part, il apparaît que la pratique du *« spamming »* est quasi exclusivement en France le fait de petites entreprises. Celles-ci utilisent les spécificités du réseau internet comme vecteur de communication. En effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau. En résumé, internet est le moyen idéal pour les entreprises disposant de faibles moyens ou offrant des services et produits à la limite de la légalité de toucher, à moindre coût, un ensemble très vaste de personnes.

Enfin, la réception des différents messages a fait apparaître que certains d'entre eux pouvaient avoir un contenu à caractère pédophile. Il a été décidé de transférer aux autorités judiciaires spécialisées dans la lutte contre ce type de criminalité l'ensemble des messages pouvant contribuer à permettre l'identification de leurs émetteurs.

C. L'action de la CNIL : fermeté et pédagogie

La CNIL n'a pas attendu la mise en place de l'opération « boîte à spams » pour s'inquiéter et travailler sur le phénomène du *« spamming ».* En effet, dès son rapport *Publipostage électronique* de 1999, elle en avait appréhendé les enjeux dans des termes que l'actualité ne dément pas.

La spectaculaire mobilisation des internautes français qu'a suscitée l'opération « boîte à spams » traduit une attente forte. L'initiative qui a été prise n'a jamais eu pour objectif de résoudre le problème du « *spamming »* dans son ensemble. Il n'en reste pas moins qu'était attendue une position sans équivoque de la CNIL. Ainsi, l'action de la Commission s'est basée sur deux idées-forces, la réalisation d'un volet pédagogique et un volet répressif — la dénonciation au parquet — afin de permettre la condamnation de certains des plus importants auteurs d'envois de messages électroniques non sollicités.

1. UN VOLET REPRESSIF ATTENDU

L'intérêt de l'opération « boîte à spams », outre l'aspect statistique évoqué plus haut qui ne relève pas spécifiquement des attributions de la CNIL, était de permettre une identification des plus grosses campagnes de *« spamming »* et de dénoncer ces pratiques qui sont manifestement contraires aux dispositions de la loi que la Commission a pour mission de faire respecter. La Commission, dès le lancement de l'opération, a indiqué qu'elle ne serait pas en mesure de donner une réponse individualisée à chacune des saisines mais qu'elle utiliserait celles-ci pour dénoncer les agissements frauduleux dont elle aurait connaissance.

a) L'analyse juridique

La pratique du « *spamming »* est susceptible en effet de constituer une pratique délictuélle en ce qu'elle enfreint certaines dispositions légales.

VIOLATION DES DISPOSITIONS DU CODE, PÉNAL RELATIVES AUX ATTEINTES AUX SYSTÈMES DE TRAITEMENT AUTOMATISE DE DONNEES

Dans sa version la plus dure, la pratique du *« spamming »* peut conduire à une forme de fraude informatique. Sans entrer dans des détails d'ordre technique, on peut relever que les émetteurs de « spams » peuvent être amenés à utiliser les ordinateurs de particuliers, à leur insu, comme outils pour un envoi massif de messages. Ainsi, un ordinateur connecté à internet par une liaison haut débit, lorsque celle-ci est mal configurée, peut servir de relais à une telle opération. Ce cas de figure n'est pas anecdotique et peut même justifier, selon les fournisseurs d'accès, une coupure d'accès au réseau lorsqu'un ordinateur, ainsi piraté, est identifié comme étant la

source de trop nombreux « spams ». L'utilisation, à l'insu des personnes, de leur matériel informatique est sanctionnée à l'article 323-1 du Code pénal[1].

Dans la même optique, le fait de pratiquer une opération de *« spamming »* qui, par l'ampleur du nombre de messages envoyés (dans un cas, 315 000 en une nuit), provoque un blocage des serveurs ou de la bande passante (on parle alors de *mailbombing)* est constitutif du délit d'entrave au fonctionnement d'un système de traitement automatisé de données prévu à l'article 323-2 du Code pénal[2] (TGI Lyon, 20 février 2001 ; tribunal correctionnel de Paris, 24 mai 2002). Sur son aspect purement informatique, la pratique du « *spamming »* est donc contraire à la législation en vigueur. Ces textes ne sont cependant applicables qu'aux cas les plus extrêmes et ne trouvent pas forcément à s'appliquer à toute opération d'envoi de courriers électroniques non sollicités.

VIOLATION DE STIPULATIONS CONTRACTUELLES

Les conditions générales d'utilisation des services d'accès à internet, telles qu'elles sont rédigées dans l'ensemble des contrats d'abonnement chez les fournisseurs d'accès, font référence au code de conduite de l'internet *(la Netiquette)* ou interdisent explicitement la pratique du *« spamming ».* Sur cette base, les fournisseurs d'accès n'hésitent alors pas à priver d'accès à internet leurs clients qui auraient été identifiés comme émetteurs de « spams ». Diverses décisions de justice[3] ont reconnu la licéité d'une telle solution, notamment en se basant sur l'article 1 135 du Code civil[4].

Cependant, ces textes ne peuvent que très rarement être invoqués par les destinataires finaux des messages qui, pourtant, en sont les premières victimes.

Paradoxalement, alors que la pratique du *« spamming »* est vivement ressentie par les internautes qui en sont victimes comme une violation de leur vie privée, rares sont les actions en justice qui ont été entreprises sur la base de la loi du 6 janvier 1978. Les fondements d'une telle action ne manquent pourtant pas.

VIOLATION DE LA LOI « INFORMATIQUE ET LIBERTÉS »

La CNIL considère qu'en principe, une adresse électronique est une information nominative[5] , les personnes qui en sont titulaires bénéficiant, en conséquence, des dispositions protectrices de la loi. Il apparaît ainsi que la pratique du *« spam-*

---

[1] Article 323-1 du Code pénal : *« le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende.*
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende ».

[2] Article 323-2 du Code pénal : « *le fait d'entraver ou de fausser le fonctionnement d'un système de traite ment* automatisé de données est puni de trois ans d'emprisonnement et de *45 000 euros d'amende ».*

[3] TGI Rochefort-sur-mer, 28 février 2001 ; TGI Paris, 15 janvier 2002.

[4] Article 1135 du Code civil : *« les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature ».*

[5] Rapport précité sur le publipostage électronique, p. 1.

ming », prise dans son ensemble, viole les dispositions de la loi « Informatique et libertés » sur au moins trois points.

En premier lieu, la méthode de collecte des adresses servant à des opérations de *« spamming »* est manifestement illicite. Les personnes victimes de cette pratique n'ont, par définition, pas communiqué à des fins de prospection leur adresse électronique aux différentes sociétés qui les sollicitent. L'analyse des « spams » reçus par la Commission et les différentes pratiques observées montrent que les entreprises à l'origine de « spams » recourent, dans l'immense majorité des cas, à des outils, appelés « aspirateurs de méls » *(robot-mails)*, permettant de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects. Cette méthode de constitution de bases de données qui revient à collecter, à l'insu des personnes, leur adresse électronique est, évidemment, en totale opposition avec l'article *25* de la loi « Informatique et libertés » qui énonce : « *la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

En second lieu, les personnes ou entreprises à l'origine de l'envoi de messages non sollicités à des fins de prospection ne permettent pas un usage effectif du droit d'opposition. Sur le modèle de l'article 26 de la loi du 6 janvier 1978, l'article 14 de la directive européenne 95/46 du 24 octobre 1995 reconnaît à toute personne le droit de s'opposer à l'utilisation commerciale de ses données ou à la transmission de celles-ci à des tiers. Ainsi, comme l'avait souligné le rapport précité de 1999, la collecte à l'insu des personnes de leurs adresses électroniques à des fins de prospection commerciale méconnaît les garanties offertes par la directive générale du 24 octobre 1995. En outre, lors de la réception de messages de type « spams », aucune possibilité n'est offerte aux internautes de s'opposer à la réception, à l'avenir, de messages similaires. Lorsque de tels liens de désinscription existent, ceux-ci sont soit inefficaces, soit ne servent qu'à « valider » l'adresse électronique utilisée, c'est-à-dire qualifier cette adresse comme étant encore valide puisqu'utilisée par son titulaire. De nombreux messages d'internautes font part à la Commission de ces problèmes. Ces pratiques de collecte et de stockage des adresses relèvent de l'article 226-18 du Code pénal[1].

Enfin, la constitution et l'utilisation de traitements automatisés d'informations nominatives doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration à la CNIL, conformément à l'article 16 de la loi du 6 janvier 1978. En effet, l'utilisation d'adresses électroniques pour mener une opération de prospection commerciale par voie électronique suppose la constitution et l'usage de traitements automatisés d'informations nominatives. Tout manquement à cette obligation est sanctionné par l'article 226-16 du Code pénal qui énonce : « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations*

[1] Article 226-18 du Code pénal : « *le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».*

nominatives sans qu'aient été respectées les formalités préalables à leur mise en *œuvre est puni de trois ans d'emprisonnement et de 45 000 euros d'amende ».*

En conclusion, la pratique du « spam » en ce qu'elle contrevient, notamment, aux principes de loyauté et de légitimité de la collecte de données personnelles est assurément contraire à la loi « Informatique et libertés ».

Un internaute victime de « spams » a ainsi porté plainte contre X devant le parquet de Paris, sur le fondement de l'article 226-18 du Code pénal. La brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI) a été chargée de l'enquête. Le jugement est attendu courant mai 2003.

b) Les dénonciations au parquet

La Commission ne peut que se féliciter de l'utilisation des dispositions de la loi du 6 janvier 1978 comme outil de lutte contre le « spam » et a décidé, au moyen d'une série de dénonciations au procureur de la République de Paris, de jouer son rôle de premier défenseur des dispositions de la loi « Informatique et libertés » lorsque celles-ci sont délibérément ignorées. L'objectif poursuivi est que cette démarche ait valeur d'exemple pour l'ensemble des entreprises se livrant à la pratique du « *spamming »* et fournisse aux internautes les moyens juridiques d'éventuelles actions de leur part.

L'action de la CNIL ne pouvant cependant s'arrêter à la dénonciation des cinq entreprises présentées ci-après, des contacts ont ainsi été pris avec certaines des entreprises françaises identifiées comme étant à l'origine de « spams » afin de leur rappeler les termes de la loi et de leur demander de cesser de telles pratiques. Certes, ces dénonciations et ces rappels à la loi ne permettront pas de tarir le phénomène du *« spamming »,* en très grande partie d'origine nord-américaine. Il s'agit cependant de porter un coup d'arrêt aux pratiques de petites entreprises françaises qui pensent avoir trouvé un créneau porteur pour augmenter leur chiffre d'affaires en collectant, en dehors de tout respect de la réglementation, des adresses électroniques à des fins de prospection commerciale.

S'agissant plus particulièrement de la méthode utilisée pour procéder à ces cinq dénonciations au parquet, la Commission a effectué une étude des messages reçus ainsi que de diverses plaintes — tant par voie postale que par voie électronique — qui ont permis d'identifier, dans la mesure du possible, un certain nombre d'entreprises à l'origine d'envois massifs et répétés de courriers électroniques non sollicités.

Quelques exemplaires de ces messages ont alors été transférés pour analyse à la direction de l'expertise informatique et des contrôles de la CNIL afin d'en déterminer l'origine ainsi que divers éléments permettant d'apprécier sans ambiguïté la réalité du caractère irrégulier de ces envois. Sur cette base, plusieurs entreprises ont été identifiées comme pratiquant du « *spamming »* selon le faisceau d'indices suivants.

D'une part, le nombre et la fréquence des messages envoyés et, par la suite, transférés par les internautes aux services de la Commission excluent l'hypothèse d'une opération de marketing classique. D'autre part, la diversité des destinataires

de ces messages (particuliers d'origines diverses, professionnels de multiples secteurs d'activité) amène à penser que les adresses de ces particuliers ont été collectées par l'utilisation d'un outil de type « aspirateur de méls », certains internautes indiquant même parfois expressément n'avoir jamais été en contact avec la société expéditrice. De plus, pour chacun des cas relevés, la possibilité de s'opposer à recevoir à l'avenir de tels messages est inexistante ou inefficace, cette dernière hypothèse étant, là aussi, confirmée de façon expresse par certains internautes. Enfin, pour les entreprises françaises identifiées, aucune formalité préalable n'a été effectuée auprès de la Commission à la date d'envoi des messages.

En conséquence, la Commission a, sur la base de ce constat, dénoncé au Parquet, sur le fondement des articles 226-16 et 226-18 du Code pénal, les entreprises suivantes : Alliance Bureautique Service (ABS), procédant à la conception et la vente de logiciels « aspirateurs de méls », Suniles agissant dans le secteur du tourisme, le Top 50 du « X » effectuant la promotion de sites pornographiques, BV Communication réalisant la promotion d'un site internet et de services minitel de rencontres, et enfin Great-Meds. corn, entreprise américaine procédant à la vente en ligne de produits pharmaceutiques.

Le choix de ces sociétés est issu d'une volonté d'identifier certaines des entreprises à l'origine de volumes d'envois les plus importants de messages non sollicités tout en opérant un panachage selon le contenu des messages reçus.

2. LE VOLET PEDAGOGIQUE : LE MODULE « HALTE AU SPAM ! »

L'un des mérites de l'opération « boîte à spams » aura été de stigmatiser la pratique du *« spamming ».* En effet, bon nombre d'internautes victimes de « spams » peuvent jusqu'à en ignorer les principales caractéristiques (son caractère illégal, son coût, comment s'en protéger, etc.) ou même avoir le sentiment que la réception des messages publicitaires non sollicités est inhérente à l'utilisation d'internet.

Dans une optique pédagogique, il est donc apparu indispensable aux yeux de la Commission de mener des auditions[1] auprès des principaux acteurs concernés par la problématique du *« spamming »,* et de manière générale par le publipostage électronique afin d'enrichir et de relayer l'action de la CNIL en matière de lutte contre le « *spamming »,* notamment en alimentant un nouveau « module » appelé « Halte au spam ! » accessible sur le site de la CNIL.

Sur le modèle de l'action qu'a entreprise la Commission pour faire prendre conscience aux internautes de la traçabilité inhérente à l'utilisation d'internet *(« Vos traces »)* ou de la protection particulière qui doit s'attacher aux mineurs *(Espace*

[1] La CNIL a constitué un groupe de travail composé de l'Association française des fournisseurs d'accès (AFA), de l'Institut national de la consommation (INC) et « 60 millions de consommateurs » et du Groupement des éditeurs de services en ligne (GESTE]. Ont également été associés à cette consultation, le Syndicat national de la communication directe (SNCD), la Fédération des entreprises de vente à distance (FEVAD) ainsi que l'Association pour le commerce et les services en ligne (ACSEL). Enfin, s'est jointe également à ce groupe de travail la délégation interministérielle à la famille (DIF).

Juniors), le site de la CNIL s'est doté d'un module à vocation pédagogique (Halte au spam !) afin d'informer les internautes des solutions, tant juridiques que techniques, qui sont susceptibles de les aider à se prémunir mais aussi à réagir à la réception de messages électroniques non sollicités. Les professionnels n'ont pas été oubliés et disposent de conseils pratiques pour procéder en toute légalité à leur campagne de prospection électronique.

a) Des conseils pratiques

S'agissant des conseils délivrés aux internautes la Commission a dans un premier temps listé les quelques réflexes de base permettant de se prémunir et de lutter contre le « *spamming* ».

Le premier consiste à faire preuve de vigilance lors de la communication de son adresse électronique. Il s'agit alors de vérifier en cas de collecte par questionnaire que celui-ci précise, outre l'utilisation qui pourra en être faite, l'existence d'un droit d'accès et de rectification, le caractère facultatif ou obligatoire des réponses, les conséquences d'un défaut de réponse et les personnes physiques ou morales destinataires des informations conformément à l'article 27 de la loi du 6 janvier 1978. Si l'adresse électronique est susceptible d'être utilisée pour le compte de tiers ou cédée à des fins, par exemple, de prospection commerciale, l'internaute doit en être informé et mis en mesure de s'y opposer en ligne au moyen par exemple d'une case à cocher.

Par ailleurs, la CNIL recommande de créer des adresses électroniques dédiées à l'achat sur internet, la communication sur les espaces publics et l'inscription à des lettres d'information et de recourir aussi souvent que possible à des pseudonymes dans le cadre des forums de discussion ou lors de l'utilisation de messageries instantanées. De plus, il est important de ne pas rendre visibles les adresses électroniques de ses correspondants lorsque l'on crée une liste de diffusion ou lors du transfert d'un message et de ne pas communiquer à un tiers des adresses électroniques sans le consentement des personnes concernées.

Enfin, il est conseillé de ne jamais répondre à un « spam » et de ne pas cliquer sur les liens hypertextes qu'il peut contenir afin d'éviter tout transfert d'information vers le « spammeur ». De même, l'utilisation d'un filtre de « spams », soit grâce aux fonctionnalités du logiciel de messagerie utilisé par l'internaute, soit par l'intermédiaire d'un logiciel spécifique, peut être préconisée.

b) Des démarches utiles

Au titre des solutions juridiques, les internautes sont informés qu'ils peuvent saisir la CNIL en joignant à leur réclamation l'en-tête du message incriminé et de préciser les démarches qu'ils auraient déjà entreprises. La Commission détaille par ailleurs la procédure à suivre afin de porter plainte directement auprès des autorités judiciaires et fournit à cet effet un modèle de lettre.

Toutefois, la Commission indique qu'il est possible d'alerter le propriétaire du serveur de messagerie utilisé par le « spammeur », l'hébergeur de son site web ou

encore que l'internaute informe son propre fournisseur d'accès à internet. Dans le même ordre d'idées les victimes de « spam » peuvent se rapprocher des organismes spécialisés dans la lutte contre le « spam ». Une partie du module « halte au spam » regroupe d'ailleurs l'ensemble des liens hypertextes permettant d'alerter les organismes et autorités compétentes ou tout simplement de s'informer. Enfin, la CNIL propose des solutions d'ordre technique devant permettre aux internautes de réagir face au « *spamming* » et en détaille la mise en œuvre, comme c'est le cas par exemple pour les différentes méthodes de filtrage des messages indésirables.

c) Des recommandations aux professionnels

S'agissant des professionnels, les recommandations portent sur la phase de collecte des adresses électroniques et sur leur utilisation. La CNIL rappelle l'ensemble des mesures à mettre en œuvre afin de respecter les droits des internautes et notamment la nécessité d'indiquer l'identité et l'adresse physique de l'éditeur du site, de préciser les finalités pour lesquelles les données sont collectées ainsi que les destinataires. Elle recommande par ailleurs, d'informer les personnes de l'existence de procédés de collecte de données automatisés tels que les « cookies », tout en soulignant que des techniques de sécurité assurant l'intégrité et la confidentialité de transmission sur le réseau des informations doivent être mises en œuvre.

Concernant les règles à respecter lors de l'utilisation des adresses électroniques, la CNIL insiste, notamment, sur l'obligation de n'utiliser à des fins de prospection commerciale que les adresses de messagerie collectées loyalement et rappelle que toute prospection électronique à destination des adresses collectées dans les espaces publics de l'internet est interdite. En outre, il est rappelé la nécessité d'offrir aux personnes concernées la possibilité de se désinscrire par tous moyens, la CNIL détaillant à cette occasion les modalités de mise en oeuvre des moyens de désinscription.

Les objectifs de l'opération « boîte à spams » ont été atteints : la réception de plus de 300 000 messages en trois mois, soit 100 000 messages par mois, démontre l'ampleur de ce qu'il faut considérer comme un véritable fléau. Au vu de ce résultat, la CNIL a engagé des actions sans précédent : cinq dénonciations à la Justice d'entreprises ayant procédé à des envois massifs de messages commerciaux non sollicités, alors que la Commission n'avait jusqu'à présent fait qu'un usage modéré de sa faculté de dénoncer au Parquet (dix-huit dénonciations de 1978 à 2001). Le caractère exemplaire de ces dénonciations devrait permettre de donner un coup d'arrêt aux pratiques des quelques entreprises françaises qui pensent pouvoir enfreindre le cadre légal en toute impunité.

Enfin, cette opération semble avoir eu un écho favorable auprès du législateur, un amendement adopté par l'Assemblée nationale en première lecture du projet de loi pour la confiance dans l'économie numérique prévoyant que la CNIL pourrait recueillir, par tous moyens y compris par courrier électronique, les plaintes relatives au non-respect des dispositions concernant la prospection directe par automate d'appel, télécopie ou courrier électronique.

II. LES « PROSPECTS » SE PLAIGNENT

A. Les plaintes depuis la fermeture de la « boîte à spams »

La fermeture de la « boîte à spams » en novembre 2002 et son remplacement par le module « Halte au spam ! » sur le site de la CNIL ne signifient pas que les victimes du « spam » sont abandonnées à leur sort. En effet, le service des plaintes de la CNIL a reçu, en 2002, plus de 160 courriers d'internautes qui reçoivent des messages électroniques non sollicités, la majorité de ces courriers ayant été adressés à la Commission postérieurement à la fermeture de la « boîte à spams ».

Ce constat témoigne du succès de cette opération qui a permis de sensibiliser les nombreux particuliers qui consultent, chaque jour, une, parfois plusieurs, boîtes aux lettres électroniques.

Quelques exemples de plaintes adressées à la CNIL illustrent les difficultés que peuvent rencontrer les utilisateurs de telles boîtes aux lettres.

Ainsi, M^me^ P. reçoit régulièrement des messages dans sa boîte aux lettres électronique l'invitant à se rendre sur un site internet édité aux États-Unis. Ce site permet de télécharger des vidéos pornographiques. Inquiète que ses enfants puissent accéder à ces messages qu'elle ne parvient pas à stopper, elle saisit la CNIL.

Les auteurs des messages électroniques non sollicités sont généralement difficiles à identifier car ils utilisent des adresses masquées par le recours à des serveurs tiers, parfois situés à l'étranger, comme dans le cas de M^me^ P. Face à de telles situations, la Commission ne peut qu'inviter l'internaute à appliquer les solutions techniques préconisées dans le module « Halte au spam ! », diffusé sur son site internet.

Dans d'autres cas, les messages reçus par les plaignants proviennent de sites internet clairement identifiables, édités par des sociétés établies sur le territoire français. La Commission intervient alors systématiquement auprès de la société éditrice du site ayant adressé le mél publicitaire afin de connaître les moyens utilisés pour collecter l'adresse électronique du plaignant et obtenir la radiation de cette adresse du fichier utilisé.

L'instruction de ces plaintes montre que, dans de nombreux cas, l'adresse électronique utilisée a été collectée directement auprès de l'internaute lors d'un achat effectué sur internet, d'une adhésion à une *newsletter* ou d'une demande de catalogue.

Si la collecte de l'adresse électronique du plaignant est rarement irrégulière, son information sur sa faculté de s'opposer à l'utilisation de ses coordonnées lors d'opérations d'e-mailing est en revanche trop souvent absente ou peu claire.

La Commission doit alors intervenir auprès de nombreux sites afin que les mentions d'information obligatoires prévues par l'article 27 de la loi du 6 janvier 1978 apparaissent sur les pages concernées des sites ou encore qu'une page dédiée à la protection des données personnelles soit mise en place.

Dès lors que l'internaute a été préalablement informé que son adresse électronique pouvait être cédée à des tiers à des fins de prospection commerciale et mis en mesure de s'y opposer par l'apposition d'une case à cocher, la Commission considère que les fichiers ainsi régulièrement constitués peuvent être mis à la disposition de tiers à des fins commerciales[1].

Enfin, d'autres plaintes mettent en évidence que, si une telle information a été réalisée, l'opposition formulée par l'internaute à ce que ses coordonnées soient utilisées à des fins de prospection commerciale par mél n'a pas été respectée. Les émetteurs de ces envois invoquent alors des « problèmes techniques » ou des « bugs informatiques ».

C'est le cas de M. L. qui reçoit régulièrement dans sa boîte aux lettres électronique des messages publicitaires de son fournisseur d'accès internet (FAI). Exaspéré par ces envois, M. L. demande à plusieurs reprises à son FAI de cesser ces envois. N'obtenant pas de réponse, il saisit la CNIL qui obtient sa radiation du fichier des envois publicitaires par mél. Quelques semaines plus tard, M. L. saisit à nouveau la Commission car les envois continuent.

La direction du FAI explique à la CNIL qu'un « bug informatique » est à l'origine d'un dysfonctionnement du processus technique bloquant les envois de messages électroniques à caractère publicitaire. Finalement, le problème a pu être réglé et M. L. ne reçoit maintenant plus de messages commerciaux de son FAI.

B. Il n'y a pas que les « spams »

Même si leur nombre baisse, les plaintes adressées à la CNIL dans le secteur du marketing direct sont encore, en 2002, les plus nombreuses. Courrier électronique on vient de le voir mais aussi téléphone, télécopie, SMS, automates d'appels : les professionnels du marketing direct ont de plus en plus d'« outils » à leur disposition.

1. INFORMER INLASSABLEMENT LES CONSOMMATEURS DES RÈGLES ET USAGES

a) Les règles

L'instruction de ces plaintes conduit la CNIL à rappeler plusieurs règles, tant aux citoyens qui la saisissent, qu'aux professionnels du marketing direct :
— la CNIL ne dispose pas des données personnelles recueillies par les organismes publics ou privés qui lui ont déclaré leurs fichiers informatisés et n'est dès lors pas en mesure de savoir dans quels fichiers est recensée une personne physique ;
— ces données personnelles sont conservées par chaque organisme (sociétés de vente à distance, sociétés éditrices de magazines ou journaux, associations...) dans leurs propres fichiers. Aucun « fichier central de consommateurs » n'existe en France ;

[1] CNIL 20e rapport d'activité 1999, p. 111.

— la loi du 6 janvier 1978 ne protège que les personnes physiques concernées par un traitement manuel ou informatisé. La CNIL ne dispose en conséquence d'aucune compétence particulière s'agissant des informations concernant des personnes mora les qui seraient enregistrées dans des fichiers ;
— la loi du 6 janvier 1978 n'interdit pas la vente, la location, l'échange — ou plus généralement, la mise à disposition — de noms et adresses enregistrés dans un fichier ;
— les consommateurs doivent être toutefois clairement informés de leur faculté de s'opposer à ce que leurs données personnelles soient mises à disposition d'organis mes extérieurs pour être utilisées à des fins de prospection commerciale ;
— ces mentions d'informations doivent figurer sur le support de collecte des données (questionnaire, bon de commande, bulletin d'abonnement, formulaire d'adhésion, demande de renseignements...). Trop souvent, ces mentions d'informations ne figu rent pas sur ces documents ;
— elles doivent apparaître clairement alors que trop souvent elles sont peu lisibles voire illisibles (taille des caractères trop petite, mention imprimée sur la tranche du document, texte peu compréhensible...) ;
— les sociétés souhaitant effectuer des opérations de prospection, par téléphone ou par courrier, auprès des abonnés du téléphone doivent respecter l'opposition à être ainsi démarchés de ceux qui se sont inscrits sur la « liste orange »[1]. Pour cela, ces sociétés doivent acquérir auprès de Wanadoo Data, filiale de France Télécom, un fichier expurgé des abonnés inscrits en listes rouge et orange ;
— la prospection par voie de télécopie ou d'automates d'appels est subordonnée à l'accord exprès et préalable de la personne démarchée[2].

Pour améliorer cette situation, la Commission diffuse un document décrivant les moyens dont dispose toute personne fichée afin d'exercer les droits qui lui sont reconnus par la loi du 6 janvier 1978 : droit de s'opposer, pour des raisons légitimes, à ce que ses coordonnées figurent dans un fichier, droit de s'opposer à ce que ses coordonnées soient utilisées à des fins de prospection, droit d'accéder aux informations qui la concernent enregistrées dans un fichier...

Par ailleurs, et afin de faciliter l'instruction des plaintes et ainsi réduire les délais de réponse, la CNIL recommande la mise en place de « correspondants CNIL » dans de nombreux organismes (sociétés de vente à distance, fournisseurs d'accès internet, opérateurs de téléphonie).

[1] L'inscription gratuite sur la liste orange interdit d'une part à France Télécom de communiquer les coordon nées de l'abonné à des fins de prospection commerciale et d'autre part, aux sociétés de prospecter direc tement à partir de l'annuaire papier ou électronique. Article R. 10-1 du Code des postes et télécommunications.

[2] Article L. 33-4-1 du Code des postes et télécommunications : « *est interdite la prospection directe, par automates d'appel ou télécopieurs, d'un abonné ou d'un utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels* ».

b) Les listes d'opposition existantes

Vous ne souhaitez pas	L'opérateur est	Vous devez vous inscrire	Coût du service
Que des organismes de VPC, de presse et de collecte de fonds vous adressent des **courriers publicitaires**	UFMD 60, rue de la Boétie 75008 Paris	Liste robinson	Gratuit
Que des sociétés de VPC et de presse vous adressent des **méls publicitaires**	FEVAD Site www.e-robinson.com	Liste e-robinson	Gratuit
Que vos coordonnées téléphoniques (n° , nom, adresse) soient publiées dans les annuaires ou communiquées par les services de renseignements	France Télécom (auprès de votre agence)	Liste rouge[1]	2,31 €/mois
	SFR (auprès de votre agence)	Liste rouge	Gratuit
	Bouygues Télécom (auprès de votre agence)	Liste privée	2,50 €/mois
	Orange (auprès de votre agence)	Pas de liste d'opposition, vous devez effectuer une démarche positive pour être inscrit	Gratuit
Que vos coordonnées téléphoniques (n° , nom, adresse) soient utilisées à des fins de prospection commerciale	France Télécom (auprès de votre agence)	Liste orange	Gratuit
Que l'on puisse retrouver votre nom ou votre adresse à partir de votre n° de téléphone (annuaire inversé)	France Télécom par simple appel à votre agence ou au 0 800 *55* 97 02 (appel gratuit)	Liste anti quidonc	Gratuit
	Iliad (« Annu »)	par simple courrier à Iliad 24, rue Emile Menier -751 16 Paris	
Que vos coordonnées téléphoniques (n°, nom, adresse) soient publiées dans les annuaires, mais vous acceptez qu'elles soient communiquées par les services de renseignements	France Télécom (auprès de votre agence)	Liste chamois	Gratuit

[1] L'inscription en liste rouge comprend systématiquement l'inscription sur la liste orange.

Vous ne souhaitez pas	L'opérateur est	Vous devez vous inscrire	Coût du service
Que vos n° de téléphone, nom et prénom apparaissent lorsque vous appelez un correspondant muni d'un appareil permettant d'identifier l'appelant	France Télécom : « secret permanent » (auprès de votre agence) ; « secret appel par appel » composez le 3651 avant les dix chiffres du n° de la personne appelée	Secret permanent ou appel par appel[1]	Gratuit
	SFR « secret permanent » (auprès de votre agence)	Liste ivoire	
	Bouygues Telecom	Appel incognito	
Que vos coordonnées soient diffusées sur les annuaires en ligne sur internet	France Télécom par simple appel au 0 800 *55* 97 02	Opposition à figurer sur le site www.pages-blanches.fr	Gratuit
	Iliad par simple courrier à Iliad Sce Annu 24, rue Émile Menier 75116 Paris	Opposition à figurer sur le site www.annu.com	
	Group'adress par simple courrier à Group'adress 92492 Sèvres Cedex	Opposition à figurer sur divers sites proposant des annuaires	

Si vous êtes client d'une société, abonné d'un journal ou magazine, adhérent ou donateur d'une association, il convient de vous adresser directement à ces organismes afin de vous opposer à ce que vos coordonnées soient mises à disposition d'autres organismes à des fins de prospection commerciale, conformément à l'article 26 alinéa 1 de la loi du 6 janvier 1978.

2. ARRETER LES DERIVES

Une publicité peut aussi révéler des « dérives » rendues possibles par le traitement automatisé d'informations nominatives à des fins commerciales. Deux exemples significatifs méritent d'être mentionnés.

M. D. téléphone régulièrement en Algérie. L'agence commerciale de son opérateur téléphonique, qui procède à l'aide d'un traitement automatisé à l'analyse de ses consommations téléphoniques, lui adresse une sollicitation lui proposant des forfaits de communications plus favorables vers les pays du Moyen-Orient et du

[1] Si vous êtes inscrit en « liste rouge » ou en « liste anti quidonc » mais que vous n'avez pas opté pour le secret permanent ou le secret « appel par appel », votre numéro - et non vos nom et prénom - est identifiable par les abonnés au service de présentation du nom.

Maghreb. Elle profite de ce courrier pour lui souhaiter « *de bonnes fêtes à l'occasion du mois du Ramadan ».*

M. D. s'étonne et saisit la Commission.

Dans ce dossier, la Commission a rappelé à l'opérateur que l'analyse des numéros appelés par l'abonné, afin de lui proposer un abonnement spécifique, ne saurait en aucun cas permettre d'établir l'appartenance, supposée ou non, des personnes à une communauté religieuse. La direction de cet opérateur s'est engagée à rappeler ces règles à ses agences commerciales afin que cesse cette pratique.

Le cas de M. F. est tout aussi parlant. Il s'inscrit sur un site internet de jeux en ligne en indiquant qu'il est un homme célibataire. Il reçoit quelque temps plus tard d'une société d'assurance une publicité vantant les caractéristiques du « *premier contrat d'assurance spécifiquement conçu pour la communauté homosexuelle ».*

Marié, père de famille, M. F. saisit la CNIL, étonné de recevoir un tel courrier.

L'instruction de cette plainte a permis d'établir que l'éditeur du site internet avait opéré un tri parmi ses clients sur la base du célibat puis édité des étiquettes-adresses qu'il a mises à disposition de cette société d'assurance.

Ce tri avait pour objet d'isoler les personnes susceptibles d'être intéressées par un produit d'assurance « spécifiquement conçu pour la communauté homosexuelle » et ainsi pour effet de permettre un traitement de données faisant apparaître les moeurs, supposées, des personnes concernées.

Or, un tel fichier est, sauf accord exprès des personnes, interdit par l'article 31 de la loi du 6 janvier 1978[1]. Toutes les données concernant M. F. ont bien évidemment été radiées du fichier de gestion de la clientèle de la société éditant le site internet, qui a indiqué qu'elle avait agi par *« maladresse »* et qu'à l'avenir de tels faits ne se reproduiraient plus.

Ce type de dérive peut avec un rappel ferme à la loi être arrêté. Il est des cas où la CNIL ne peut se borner à y mettre fin et où elle doit aller plus loin dans l'utilisation des moyens juridiques dont elle dispose.

3. UN USAGE PERVERTI DU SMS

Le succès du SMS *(Short Message System)* comme nouveau moyen de communication n'a pas manqué de créer un nouveau mode de prospection. Le SMS est un message texte recevable sur téléphone mobile avec une capacité limitée tant dans sa taille (160 caractères) que dans son stockage dans la carte mémoire du téléphone (seuls 10 SMS environ peuvent y être stockés).

[1] Article 31 de la loi du 6 janvier 1978 : *« il est interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de l'intéressé, des données qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs* des personnes ».

a) Billet doux

La CNIL a été saisie, au cours des mois de mai et juin 2002, d'un nombre important de plaintes ou de demandes de renseignements relatives à des opérations de prospection par SMS invitant les personnes démarchées à appeler un numéro audiotel afin de s'y voir communiquer un message. Concrètement, ces personnes recevaient un SMS qui énonçait, par exemple : « *Quelqu'un t'aime en secret et nous a chargés de te prévenir, devine qui a flashé sur toi en appelant le 08 7,35 euro/appel + 0,34 euro/min ».*

La majorité des plaintes reçues a résulté d'un envoi massif et spontané de SMS dans le seul but de générer des appels sur un numéro audiotel sans qu'aucun tiers ne soit à l'origine de cet envoi qui procédait exclusivement d'une volonté commerciale des sociétés en cause. De plus, lorsque les destinataires de ces messages ont rappelé le service audiotel pour savoir qui pouvait être à l'origine de ces messages, il leur était généralement demandé de saisir les numéros de téléphone de ceux de leurs amis qu'ils estimaient pouvoir être à l'initiative de cet envoi. Ce faisant, l'opérateur enrichissait sa base de numéros de téléphone valides.

Selon la DGCCRF (direction générale de la concurrence, de la consommation et de la répression des fraudes) qui avait alors été contactée par les services de la Commission, trois millions de SMS ont été envoyés pour le seul département des Hauts-de-Seine générant, en retour, plus de 1 80 000 appels vers les numéros audiotel indiqués.

Ce type d'opération de prospection est néfaste à plus d'un titre, notamment par son caractère intrusif et, en quelque sorte, dolosif qui risque de jeter un discrédit durable sur les modèles économiques classiques utilisant le SMS dans le cadre légal.

b) Analyse juridique

Lorsqu'elle a été saisie de cette affaire, la Commission a considéré que l'envoi d'un nombre important de SMS pouvait être assimilé à l'utilisation d'un automate d'appel. Il faut rappeler que les ordonnances de juillet et août 2001 transposant certaines dispositions des directives européennes relatives aux télécommunications et à la vente à distance subordonnent la prospection par automates d'appel et télécopies au consentement préalable des personnes.

Cette position a été confortée et précisée par la directive « vie privée et communications électroniques » du 12 juillet 2002 qui prévoit dans son article 13.1 que *« L'utilisation de* [...] *courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable* ». La directive considérant un « courrier électronique » comme *« tout message sous forme de texte […] envoyé dans un réseau public de communications qui peut être stocké dans l'équipement terminal du destinataire »,* la prospection par SMS devrait sous peu être soumise à un régime dit d'« *opt-in ».* Cette disposition est en cours de transposition dans le projet de loi relatif à la confiance dans l'économie numérique (voir *infra).* Néanmoins, lors de l'instruction des plaintes relatives à cette

opération de prospection, le cadre juridique n'était pas aussi précisément défini et, surtout, sa méconnaissance n'était pas pénalement sanctionnée.

La Commission n'a cependant pas eu à s'appuyer sur les textes applicables aux opérations de prospection par SMS pour juger du caractère illégal de ces opérations. En effet, ces dernières se trouvent en violation avec un certain nombre des dispositions légales relatives à la protection des données personnelles.

Il apparaît, selon les informations fournies par la DGCCRF et certains des opérateurs, que les envois de SMS étaient basés, d'une part, sur une composition aléatoire de numéros de téléphone et, d'autre part, sur des fichiers de numéros achetés.

La Commission a toujours considéré que la composition aléatoire de numéros de téléphone ne soumettait pas, en tant que telle, l'appelant aux dispositions de la loi du 6 janvier 1978. C'est cette position qui a été constamment appliquée au profit des instituts de sondage qui, notamment en matière politique, procèdent très fréquemment selon cette méthode.

Néanmoins, l'envoi massif de SMS à partir de ces numéros composés aléatoirement ne sert que d'accroché pour, dans un deuxième temps, permettre de récupérer auprès des personnes des numéros de téléphone valides. Concrètement, les personnes appelant ce type de service se voient demander, sous un prétexte le plus souvent fallacieux ou pour le moins trompeur — dans la mesure où personne d'autre que l'entreprise commerciale concernée ne leur a délivré un message —, de communiquer les numéros de téléphone de leurs proches. On trouve là une nouvelle variante de la technique du marketing viral qui sera évoquée plus loin dans ce chapitre.

Une telle opération de collecte de numéros de téléphone est incontestablement déloyale en ce qu'elle repose sur une incitation mensongère à la curiosité. D'autant plus lorsque la facturation de l'appel est élevée.

Ainsi, dès lors qu'une entreprise commerciale ayant adressé des SMS, collecte en retour auprès de la personne appelant son service audiotel plusieurs numéros de téléphone, sous couvert de devinette *(« A votre avis, qui a pu vous envoyer un tel message ? Veuillez taper trois numéros de téléphone et nous vous dirons si vous avez gagné ! »),* il y a donc collecte déloyale ou illicite de données personnelles, en l'espèce les numéros de téléphone de tiers, ce qui constitue le délit prévu par l'article 226-18 du Code pénal.

L'opération consistait, pour les entreprises commerciales concernées, non seulement à s'enrichir en attisant faussement la curiosité de tiers, mais aussi à constituer un fichier de numéros de téléphone portables à moindre frais.

Aucune des entreprises concernées n'avait jamais déclaré auprès de la CNIL un traitement automatisé d'informations nominatives de collecte de numéros de téléphone par de tels procédés, ce qui les met en infraction avec les dispositions de l'article 226-16 du Code pénal.

Au total, sans qu'il soit même besoin de se prononcer sur les éventuelles violations du droit de la consommation, il est évident que les opérations de prospections

massives par SMS telles que décrites ci-dessus contreviennent aux règles relatives à la protection des données personnelles.

c) Dénonciation au parquet

Compte tenu de l'écho de cette affaire, de la dérive qu'elle illustre sur des méthodes commerciales non seulement contestables mais irrégulières, la Commission a décidé, par une délibération en date du 27 juin 2002, de dénoncer au parquet, sur le fondement des articles 226-16 et 226-18 du Code pénal, les entreprises qui, à l'occasion d'un envoi massif et spontané de SMS, ont collecté de manière déloyale des données et n'ont pas satisfait aux obligations déclaratives. Prenant en compte la difficulté d'identifier précisément la ou les sociétés à l'origine de ces opérations, la Commission s'est contentée de constater les faits décrits ci-dessus, de les qualifier pénalement, tout en les portant à la connaissance du parquet, accompagnés des numéros de téléphone permettant d'identifier les services audiotel concernés, en laissant le soin aux autorités compétentes d'identifier les auteurs des infractions.

Cette position, forte, a permis à la Commission d'affirmer son attachement à ce que le développement des nouvelles techniques de prospection — quel qu'en soit le contenu — se fasse dans le respect des dispositions de la loi « Informatique et libertés ». De plus, elle marque la distinction qui doit être faite entre ceux des opérateurs qui peuvent être amenés à saisir la CNIL d'un dossier de déclaration lui demandant son avis ou ses recommandations sur les bonnes pratiques, et les autres qui, dans le mépris total de la loi, ont abusé de nombreux consommateurs tout en réalisant un chiffre d'affaires considérable.

4. DETOURNEMENT D'ANNUAIRES

La Commission a été saisie de plaintes concernant l'utilisation par deux sociétés d'annuaires d'anciens élèves de grandes écoles. La première société commercialise sur internet auprès de cabinets de conseil en recrutement un accès à sa base de données regroupant des informations concernant d'anciens élèves. La seconde utilise le même type d'informations à des fins de prospection commerciale pour les services qu'elle propose (conseils dans le domaine fiscal).

Les personnes démarchées se sont retournées vers les associations d'anciens élèves dont elles dépendent qui, par l'intermédiaire de leur représentant, ont saisi la Commission.

Les éléments des saisines ont fait apparaître que les deux sociétés en cause ne pouvaient se prévaloir d'aucun accord avec les associations d'anciens élèves dont elles utilisent les annuaires. Dès lors, les associations n'ont pu transmettre à ces sociétés les oppositions à la cession qu'elles avaient recueillies auprès des anciens élèves lors de la constitution des annuaires. Il semble en fait que les fichiers mis en cause aient été le résultat d'opérations consistant à scanner les annuaires papier des associations d'anciens élèves.

a) Le droit d'opposition en cause

Le mode de collecte des données ci-dessus exposé se trouve en contradiction avec certaines dispositions de la loi du 6 janvier 1978.

Certes, les cessions ou mises à disposition de fichiers ne sont pas interdites par la loi et cette pratique est courante en matière de marketing. Comme le précise la Cour de Cassation dans son arrêt du 25 octobre 1995[1], *« la loi du 6 janvier 1978 ne fait nulle obligation au responsable du fichier qui recueille auprès de tiers des informations nominatives aux fins de traitement d'en avertir la personne ».* En revanche, l'information est faite au moment de la collecte des données.

Le comportement fautif réside ici dans le fait de recueillir des informations concernant une personne qui se serait opposée à une telle cession.

En effet, une personne a pu lors de son inscription sur un annuaire s'opposer légitimement, conformément à l'article 26 de la loi du 6 janvier 1978, à toute transmission à des tiers des informations la concernant.

b) Avertissement

L'instruction des saisines a permis d'établir qu'une des sociétés avait, dès 1998, procédé à une déclaration de traitement automatisé d'informations nominatives ayant pour finalité la « recherche de candidats par les cabinets de recrutement ». Lors de l'instruction du dossier, l'attention du déclarant avait déjà été attirée sur le caractère déloyal et illicite de la collecte des informations. La Commission a donc rappelé à cette société les observations qui lui avaient déjà été faites, tout en lui demandant des précisions sur les conditions d'exercice par les personnes de leur droit d'accès. Les contacts avec cette société se poursuivent afin de faire respecter les dispositions de la loi « Informatique et libertés ».

Concernant la seconde société, aucune déclaration n'avait été faite lors de la saisine de la Commission. Informée de l'obligation de déclaration issue de l'article 16 de la loi du 6 janvier 1978, cette société a procédé à une déclaration en référence à la norme simplifiée n° 11 (déclaration simplifiée concernant les traitements automatisés d'informations nominatives relatifs à la gestion des fichiers de clients actuels et potentiels). Par ailleurs, le caractère déloyal de la collecte a été précisé à la société qui n'a pas répondu aux différents courriers qui lui ont été envoyés. Prenant acte du silence de cette société et des manquements constatés, la Commission a décidé, par une délibération n° 02-065 en date du 24 septembre 2002, d'adresser un avertissement à la société en cause. Suite à cette décision, *cette* société s'est engagée à ne plus démarcher les personnes inscrites dans les annuaires ayant été à l'origine des plaintes et, d'une manière plus générale, à informer les écoles ou associations d'anciens élèves, lors de l'acquisition des annuaires qu'elles éditent, de l'utilisation à des fins de prospection commerciale qui en sera faite afin de respecter le droit des personnes qui y sont inscrites.

[1] Cass. Crim., 25 octobre 1995, *Bernard R. et GIE.*

Enfin, la Commission a décidé de rappeler aux différentes écoles ou associations d'anciens élèves les termes de sa délibération du 8 juillet 1997 relative aux annuaires des abonnés au téléphone, valable pour tout type d'annuaire.

III. DE NOUVELLES PROBLEMATIQUES

Science du marketing et technologies de l'information ne cessent de se croiser pour générer des usages, des produits ou des projets qui interpellent la CNIL.

A. « Le marketing viral »

On entend par « marketing viral » la promotion d'un bien ou d'un service par les utilisateurs eux-mêmes, caractérisée par un faible coût pour l'entreprise concernée et un fort potentiel de fidélisation en cas de succès. Les moyens utilisés sont nombreux (cartes postales virtuelles, communautés, publicités « décalées »...) et le développement de ce nouveau type de marketing est rapide.

À titre d'illustration, on peut citer un traitement dont la Commission a reçu la déclaration, relatif à l'envoi de messages humoristiques sur les messageries vocales de téléphones portables.

Ce traitement concernait la mise en place, pour une période déterminée, d'un service permettant d'appeler, depuis un téléphone fixe ou mobile, un serveur vocal afin de choisir un message humoristique et de le déposer sur la messagerie vocale d'un téléphone portable d'une personne de son choix. Les seules informations indirectement nominatives, au sens de l'article 4 de la loi du 6 janvier 1978, qui étaient traitées par la société étaient le numéro de téléphone de l'appelant et le numéro de téléphone de l'appelé. Le message humoristique délivré ne comportait aucune indication de nature publicitaire et ne faisait état ni du nom de la société à l'origine de cette opération, ni de l'identité de l'expéditeur du message.

Il convient de noter que la personne destinataire du message, dont la curiosité avait immanquablement été excitée, était mise immédiatement en communication avec le service consommateur de la société éditant ce service, si elle consultait l'historique de ses messages et utilisait la fonction « rappel ». De plus, le « bouche à oreille » aidant, surtout parmi le jeune public, véritable cœur de cible de l'opération, le service consommateur de l'entreprise pouvait être directement appelé par tel ou tel destinataire du message.

Les personnes ne désirant plus recevoir ce type de message pouvaient s'inscrire sur une liste d'opposition gérée par l'entreprise éditrice.

Les informations collectées (numéros de téléphone de l'appelant et du destinataire) étaient conservées jusqu'à la fin de l'opération.

La Commission a analysé ce type d'opération non comme une opération de prospection à proprement parler mais comme une opération de « parrainage » dans laquelle une personne communique à un opérateur commercial les coordonnées d'une autre personne avec laquelle cet opérateur va dès lors pouvoir entrer en communication. Il convient de rappeler que la CNIL recommande, en matière de parrainage, que l'identité du parrain figure systématiquement sur le premier document adressé à la personne qu'elle a parrainée. Les associations professionnelles se sont d'ailleurs ralliées, dans leur code de déontologie, à une telle manière de faire.

Dans la mesure où le numéro de téléphone de la personne destinataire du message allait être communiqué à la société déclarante, conservé et traité par elle, le traitement de cette information devait répondre aux exigences de la loi et tout particulièrement à l'exigence de loyauté.

Or, dans le cas d'espèce, le destinataire du message qui n'avait rien sollicité de quiconque allait voir son numéro de téléphone communiqué, à son insu, à la société éditrice de ce service, et conservé par elle. Toujours passif, il aurait écouté le message humoristique qui lui avait été adressé de manière anonyme ; se demandant quel en est l'expéditeur, il aurait consulté le fichier historique des appels reçus et aurait rappelé immanquablement ce numéro, d'autant plus innocemment que le message délivré aurait été dépourvu de toute connotation commerciale, pour tomber alors sur le service client de la marque.

Sur le seul terrain de la loyauté de la collecte et du traitement d'une information personnelle (en l'espèce les numéros de téléphone des destinataires des messages), la CNIL a donc appelé l'attention du déclarant sur le fait que les personnes souhaitant envoyer un message humoristique à un tiers doivent préalablement s'assurer de l'accord des destinataires pour que leur numéro de téléphone soit communiqué et traité par une entreprise avec laquelle ils n'entretiennent aucun contact.

Par ailleurs, conformément aux préconisations de la Commission en matière de parrainage, les personnes destinataires des messages humoristiques doivent être informées de l'identité de l'expéditeur. Ces dispositions sont reprises dans le code de déontologie des professionnels du marketing direct.

Enfin, le principe de finalité a conduit à appeler l'attention du déclarant sur le fait qu'en aucun cas, les numéros de téléphone collectés — ceux des appelants et ceux des destinataires — ne pouvaient être utilisés à d'autres fins que la délivrance du message humoristique, et ne pouvaient donc pas l'être à des fins de prospection plus directe des personnes ou être cédés à des fins commerciales à des tiers.

Ces observations ont été portées à la connaissance de l'entreprise concernée et du prestataire technique qui proposait ce service, ce dernier s'étant alors engagé à notifier ces préconisations aux futures entreprises clientes de son service de messagerie.

B. La base centralisée du groupe Vivendi Universal

L'examen de la déclaration déposée en février 2002 par le groupe Vivendi Universal relative à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité principale « la réalisation et la gestion d'opérations de marketing » a été l'occasion pour la CNIL de poursuivre sa réflexion sur les garanties qui doivent être apportées aux échanges de données entre sociétés d'un même groupe.

La Commission suit ce phénomène depuis plusieurs années tant dans le secteur bancaire qui a transformé ses applicatifs informatiques pour avoir une vision globale de la clientèle que pour de grandes entreprises qui ont des projets de marketing relationnel (en anglais marketing « *one-to-one* » ou CRM de « *Customer Relationship Management* »).

Il est symptomatique de constater que ces outils sont désormais utilisés non plus au niveau d'une entreprise mais de groupes. C'est ainsi qu'à quelques mois d'intervalle, la CNIL a été saisie ou informée de deux autres grands projets, à savoir le programme « Byzance » mis en place par le groupe Pinault — Printemps — La Redoute et le projet Alliance développé par le groupe Galeries Lafayette et le groupe Casino. Cependant, les différences entre ces trois projets sont d'importance. Dans le cas de Vivendi Universal, il s'agissait d'une gestion de base centralisée alors que les deux autres projets portaient sur la gestion de base croisée. De plus, les projets Byzance et Alliance sont des programmes de fidélisation qui reposent sur le consentement et l'adhésion des clients alors que pour Vivendi Universal, les seuls clients qui figurent dans la base marketing, sont ceux qui ne se sont pas opposés à une cession à des fins commerciales. À cet égard, la CNIL réalise une étude d'ensemble sur les différents usages et systèmes de gestion personnalisée de la clientèle, tant auprès des associations de professionnels du marketing, des sociétés utilisatrices que des concepteurs de logiciels afin de doter la Commission d'un dispositif de réflexion approfondie sur le sujet. Cette étude se poursuit en 2003.

À finalité exclusivement marketing, le nouveau fichier présenté par le groupe Vivendi Universal avait pour objectif principal la constitution d'une base de données commune à différentes sociétés françaises du groupe Vivendi Universal. Il était ainsi envisagé de procéder à une « mutualisation » des bases de données clients des entités françaises du groupe ayant adhéré volontairement au programme afin d'enrichir la connaissance du client et de favoriser les opérations de marketing croisées et d'aboutir ainsi à une fiche « client Vivendi Universal ».

La CNIL avait rappelé à l'occasion de la mission de contrôle effectuée auprès de Canal+ (délibération n° 01-040 du 28 juin 2001, *cf.* 22e rapport d'activité 2001), société appartenant au groupe Vivendi Universal, qu'aucune disposition de la loi « Informatique et libertés » n'interdit de vendre ou de céder un fichier à un tiers dès lors que les informations ne sont pas couvertes par un secret particulier, tel que le secret médical ou le secret bancaire. En revanche, une telle cession ne peut intervenir qu'à la condition que les personnes concernées aient été préalablement informées d'une telle éventualité et mises en mesure de s'y opposer, simplement et gratuitement (article 14 de la directive de 1995). Cette condition qui est une garantie

essentielle doit être réalisée dans tous les cas et encore convient-il que cette information soit faite clairement.

La délibération Canal+ a également affirmé le principe qu'un groupe de sociétés réunissant des entités juridiquement distinctes, dont certaines peuvent exercer des activités tout à fait différentes, ne saurait, au seul motif des liens en capital, réaliser une base de données commune à partir de bases constituées pour des fins différentes sans souci du droit que les personnes tiennent des législations de protection des données personnelles. Le groupe Vivendi était en effet susceptible de constituer un fichier de 70 millions d'abonnés tous médias confondus (télévision, internet, téléphone) dont un grand nombre pouvait être clients de plusieurs sociétés appartenant au groupe Vivendi. Pour exemple : *« j'ai un portable SFR, je lis* l'Express *et je suis abonné à Canal+ ».* C'est bien le recoupement de toutes ces informations dans une base unique qui fait naître des risques.

C'est ainsi que la Commission a considéré, lors de sa séance du 30 mai 2002, que la mise en œuvre d'une base de données commune à des fins exclusivement marketing devait être accompagnée de garanties spécifiques.

Il a été rappelé que le choix technique d'une base de données centralisée résultant du regroupement de données personnelles provenant des fichiers des différentes filiales du groupe constitue un traitement nouveau, distinct de chacun des traitements mis en œuvre par les filiales.

La Commission a considéré qu'un tel schéma d'organisation du traitement de l'information nécessitait, en application de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive 95/46 du 24 octobre 1995, que les personnes concernées soient informées, préalablement à toute cession au groupe de données les concernant, de l'existence de ce fichier centralisé et du droit dont elles disposent de s'opposer à une telle cession.

S'agissant de l'exercice par les personnes concernées de leur droit de s'opposer au regroupement des données les concernant dans une base commune placée sous la responsabilité de la société Vivendi Universal, la Commission a préconisé l'apposition d'une case à cocher sur tout support de collecte des informations.

En outre, la Commission a estimé que la société Vivendi Universal devait, en tant que telle, apparaître explicitement au titre des destinataires, les données en cause devant être rassemblées avec d'autres dans une base placée sous sa responsabilité.

De même, les personnes qui, préalablement informées de leur droit d'opposition, ne l'auraient pas exercé et auraient ainsi consenti à ce que la société Vivendi Universal puisse disposer des données les concernant doivent être en mesure d'exercer leur droit d'accès et de rectification à l'ensemble des informations contenues dans la base centralisée.

Ces préconisations n'ont finalement pas eu à s'appliquer dans la mesure où Vivendi Universal a décidé à la fin de l'année 2002, compte tenu des restructurations opérées au sein du groupe, de mettre un terme à ce projet de base commune.

IV. LES RÈGLES DU JEU

A. La concertation avec les professionnels : le code de déontologie de l'e-mailing

Comme cela a été fait à de multiples reprises, notamment avec la FEVAD pour « labelsite » et compte tenu de l'attention toute particulière que la Commission porte aux garanties reconnues aux personnes en matière de prospection par courrier électronique, a été examiné le 23 avril 2002 en séance plénière le code de déontologie de l'e-mailing élaboré par le Syndicat national de la communication directe (SNCD). Ce syndicat professionnel regroupe les acteurs spécialisés dans la chaîne logistique de la communication directe comme par exemple les courtiers et propriétaires de fichiers, les sociétés de services informatiques pratiquant le traitement d'adresses, les fabricants d'enveloppes et les prestataires de l'e-mailing.

La Commission a considéré que les dispositions sur la protection des données personnelles et de la vie privée contenues dans ce code étaient conformes aux exigences légales et aux préconisations de la CNIL. En effet, tous les principes généraux qui régissent la protection des données personnelles sont rappelés et les modalités pratiques de leur mise en oeuvre par les professionnels sont précisées au moyen des préconisations de la CNIL en la matière, à savoir la reprise de mentions d'information proposées par la CNIL.

Ce code prévoit notamment qu'une adresse de courrier électronique ne peut être utilisée à des fins marketing que si la personne auprès de laquelle elle a été collectée a été mise en mesure, au moment de la collecte, de consentir ou de s'opposer à une telle utilisation. Sur ce point, il peut être remarqué que le code avait choisi d'anticiper la législation européenne issue de la directive du 12 juillet 2002 dite « Vie privée et communications électroniques » qui subordonne la prospection par courrier électronique au consentement préalable des personnes concernées.

Le code comprend également des dispositions spécifiques s'agissant de la collecte de données auprès de mineurs qui reprennent les recommandations formulées par la Commission dans son rapport d'ensemble relatif à « Internet et les mineurs » *[cf.* 22e rapport d'activité), comme par exemple, ne pas collecter à travers un mineur les données relatives à autrui ou encore ne collecter que les données strictement nécessaires à la finalité du traitement. Enfin, il reprend intégralement les propositions faites par la CNIL s'agissant des dispositions relatives aux flux transfrontières et au droit national applicable. À cet égard, le code de déontologie préconise l'emploi des clauses contractuelles types adoptées par la Commission européenne dans ses deux décisions du 15 juin 2001 (concernant les transferts de données entre deux responsables de traitement) et du 27 décembre 2001 (concernant les transferts de données d'un responsable de traitement vers un sous-traitant).

Ce code prévoit ainsi un dispositif concret et efficace qui apporte une réelle valeur ajoutée aux principes légaux existants. La CNIL a d'ailleurs toujours considéré que ce type d'initiative professionnelle devait être approuvé et encouragé dans la mesure où cela contribue à une meilleure application des dispositions de protection

des données. La mise en place de codes de déontologie permet en effet de relayer l'action de sensibilisation de la CNIL et de diffuser plus largement la culture « Informatique et libertés » auprès des professionnels du secteur du marketing direct par e-mail.

B. L'avis de la CNIL sur le projet de loi relatif à l'économie numérique

Le gouvernement a saisi la CNIL le 18 novembre 2002 de l'avant-projet de loi relatif à la confiance dans l'économie numérique qui assure notamment la transposition des dispositions relatives aux communications électroniques non sollicitées issues de la directive européenne « Vie privée et communications électroniques » du 12 juillet 2002[1].

1. LE PRINCIPE DU CONSENTEMENT PREALABLE

Cette directive, qui abroge et remplace la directive 97/66 CE du 15 décembre 1997, subordonne l'utilisation de courriers électroniques dans les opérations de prospection directe au consentement préalable des personnes concernées.

La prospection opérée par courrier électronique doit dorénavant se faire dans les mêmes conditions que celles fixées pour la prospection par télécopie et par automates d'appel. Pour mémoire, le dispositif juridique applicable à ces modes de prospection résulte de deux ordonnances des 25 juillet et 23 août 2001 insérant respectivement un nouvel article L. 33-4-1 dans le Code des postes et des télécommunications et un nouvel article L. 121-20-5 dans le Code de la consommation (cf 22e rapport d'activité, p. 30).

Le législateur européen a finalement tranché en faveur d'un régime de consentement préalable *(opt-inj* en matière de prospection par courrier électronique, solution approuvée par la CNIL dans la mesure où elle est de nature à assurer de manière plus satisfaisante la protection des données personnelles, le respect de la vie privée et la tranquillité des personnes. La CNIL avait en effet souligné dans son avis sur le projet de loi sur la société de l'information rendu le 3 mai 2001 (cf. 21e rapport d'activité, p. 21) les difficultés pratiques de mettre en place des registres d'opposition à la prospection par courrier électronique.

Le texte assurant la transposition de ce nouveau dispositif — adopté en première lecture par l'Assemblée nationale le 26 février 2003 — reprend en grande partie les observations formulées dans l'avis de la Commission.

Ainsi, il ressort de l'examen des articles 10 à 13 du projet de loi relatifs au cadre juridique de la publicité en ligne par voie électronique et notamment celle

[1] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

opérée par courrier électronique que, comme l'avait préconisé la Commission dans son avis :
— le terme de « non sollicitées » de l'article 11 insérant un nouvel article L. 121-15-1 du Code de la consommation a été supprimé, permettant ainsi de faire peser l'obligation d'identification d'une démarche publicitaire sur l'ensemble des courriers électroniques qui peuvent être reçus par une personne ;
— l'alinéa 3 de l'article L. 33-4-1 du Code des postes et des télécommunications qui interdit le fait de ne pas indiquer d'adresse valable que le destinataire du message peut utiliser en retour ainsi que le fait de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise a été clarifié ;
— le terme de « courrier électronique » a été défini. Le législateur a repris la défini tion issue de l'article 2 de la directive du 12 juillet 2002 permettant ainsi d'assurer la « neutralité technologique » du dispositif. Sont donc inclus dans la définition de cour rier électronique les SMS *(« Short Message Service »)* et les MMS *(« Multimedia Messaging Services »)* ;
— enfin, un régime transitoire a été instauré prévoyant que jusqu'à la date d'entrée en vigueur de la loi (le 31 octobre 2003), les informations relatives aux clients ou prospects pourront être utilisées afin d'offrir à ces derniers la faculté d'exprimer leur consentement à de futures opérations de prospection directe.

2. LA PORTEE DE LA DEROGATION

La CNIL avait également souhaité que la dérogation au consentement préalable en matière de prospection directe par voie électronique soit limitée à la sphère marchande. En effet, le nouveau dispositif prévoit, à certaines conditions très restrictives, la possibilité d'effectuer une prospection par courrier électronique sous réserve du respect du droit d'opposition des personnes concernées. La Commission avait à cet égard préconisé, dans le souci d'une meilleure protection des personnes, une rédaction de cette dérogation identique à celle adoptée par le législateur européen (article 13 de la directive), choix qui n'a finalement pas été repris par l'Assemblée nationale. Le texte adopté en première lecture permet de faire bénéficier de cette dérogation, non plus uniquement le secteur marchand (comme le laisse penser la rédaction de la directive) mais aussi le secteur non marchand (le projet de loi vise les personnes ayant fourni « une vente ou une prestation de service »).

En outre, la CNIL a fait observer que ce nouveau dispositif, s'il accorde un niveau de protection élevé en exigeant le consentement préalable des personnes, est de nature à soulever, tant dans son champ d'application que dans son interprétation, des difficultés d'application.

En premier lieu, s'agissant de la dérogation au consentement préalable en matière de prospection directe par courrier électronique, elle ne peut s'appliquer que si la prospection concerne des « produits ou services analogues » à ceux fournis par la même entité commerciale qui a recueilli les coordonnées électroniques du démarché.

L'ambiguïté sur l'étendue exacte de cette notion est source d'incertitude. En effet, le concept de « produits et services analogues », s'il s'inscrit dans une dérogation par ailleurs strictement encadrée, est source d'interprétations qui ne manqueront pas d'être divergentes selon les entreprises. A titre d'exemple, l'opération qui consiste à acheter en ligne un livre autorise-t-elle le vendeur à prospecter l'acheteur pour un disque (un disque est-il un « bien » analogue à un livre ?) ou pour un voyage (acheter un voyage en ligne est-ce un « service » analogue à l'opération d'acheter un livre en ligne ?). Les risques d'interprétations divergentes existent et elles se feront au détriment, d'une part, de la sécurité juridique et, d'autre part, de la protection des données personnelles des individus, avant l'établissement d'une jurisprudence. C'est pourquoi la CNIL a préconisé une interprétation stricte de l'étendue de la dérogation, sous peine de voir la prospection directe par courrier électronique rester dans un régime de droit d'opposition. Dans l'exemple cité ci-dessus, un disque peut être analysé comme un produit similaire à un livre (notion de bien culturel) alors qu'une proposition de voyage est sensiblement différente.

Par ailleurs, le dispositif communautaire issu de la directive du 12 juillet 2002 laisse le choix aux États membres, quant au champ d'application du principe du consentement préalable, de l'étendre ou non aux personnes morales.

Dans un premier temps, il avait été choisi d'appliquer ce dispositif aux personnes morales, la CNIL s'étant d'ailleurs félicitée de ce choix qui évitait la délicate opération qui aurait consisté à distinguer les coordonnées électroniques des personnes physiques de celles des personnes morales.

Cependant, cette position a été partiellement remise en question suite à l'adoption du texte par l'Assemblée nationale. En effet, le principe du consentement préalable des personnes physiques et morales a été maintenu pour les opérations de prospection opérées par automates d'appel et télécopieurs. En revanche, s'agissant de la prospection par courrier électronique, le législateur français a, en l'état actuel du texte portant transposition, choisi d'opérer une distinction au sein des personnes morales entre celles non inscrites au répertoire du commerce et des sociétés (RCS) qui bénéficient du principe du consentement préalable, et les autres qui restent sous le régime légal précédent (dit *« opt-out »).* Ce choix qui est destiné à assurer un niveau de protection maximum aux artisans et professions libérales pose à nouveau la délicate question de la distinction des adresses électroniques utilisées par les personnes qui bénéficient du régime du consentement préalable et celles qui bénéficient du régime du droit d'opposition.

Afin de trouver des solutions concrètes aux problèmes posés par ce nouveau dispositif, la Commission a participé notamment à des groupes de travail réunissant des professionnels du marketing électronique (par exemple, « L'observatoire du mail » mis en place par l'ACSEL (Association pour le commerce et les services en ligne) et l'IREPP (Institut de recherches des Études et prospective postales) qui étudient des solutions aux questions que se posent les acteurs du secteur.

3. LA MISE EN PLACE DE LA NOUVELLE REGLEMENTATION

La CNIL a également souhaité que soient définies à l'échelle européenne, et après consultation des autorités de contrôle, des lignes directrices qui permettraient d'harmoniser la mise en œuvre de ce dispositif. Ce travail pourrait être entrepris dans le cadre du groupe dit de « l'article 29 » dont une des missions est de contribuer à une application homogène de la législation européenne relative à la protection des données personnelles.

Enfin, sur le modèle des exemples d'informations à fournir aux internautes sur leurs droits lors de la mise en ligne d'un site web, la CNIL envisage de mettre à disposition notamment des professionnels du marketing un guide pratique présentant les modalités selon lesquelles peuvent être collectées et utilisées des données à caractère personnel dans le cadre d'opérations de prospection par voie électronique. À cette fin, la CNIL entend se rapprocher des professionnels de ce secteur afin d'élaborer des exemples de mentions d'informations conformes au système dit d'« *opt-in ».* Elle envisage notamment de travailler avec le Syndicat national de la Communication directe qui l'avait saisi de son code de déontologie de l'e-mailing qui prévoyait déjà les modalités de recueil du consentement *(cf. supra).*

Ce guide pratique « opt-in » complétera ainsi le module pédagogique « Halte au spam ! » élaboré par la CNIL à l'occasion de son opération « boîte à spams » qui dispense des conseils pratiques à l'attention des professionnels réalisant des opérations de publipostage par courrier électronique *(cf. supra].*

À cet égard, il faut souligner que le projet de loi intègre un nouvel alinéa 3 à l'article L. 33-4-1 du Code des postes et des télécommunications qui définit le consentement selon les termes posés par l'article 2 de la directive du 24 octobre 1995. Celui-ci dispose que le consentement de la personne s'entend par « toute *manifestation de volonté, libre, spécifique et informée, par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».* L'insertion de ce nouvel alinéa est de nature à réaffirmer la portée du consentement dans les opérations de prospection qui exclut, comme l'a indiqué la CNIL dans son avis, que son expression soit par exemple diluée dans une acceptation des conditions générales d'un service proposé. La CNIL recommande que le recueil du consentement soit effectué par exemple par le biais d'une case à cocher, comme le suggère l'un des considérants de la directive du 12 juillet 2002, et elle rappelle à ce titre que l'apposition d'une case pré-cochée est contraire à l'esprit du texte ainsi qu'au principe de loyauté de la collecte.

Enfin, comme cela a déjà été signalé, le projet de loi introduit un nouvel alinéa 7 à l'article L. 33-4-1 du Code des postes et des télécommunications qui consacre la mise en place au sein de l'autorité de protection d'une boîte aux lettres électronique qui recueillerait les plaintes relatives au non-respect des dispositions applicables aux opérations de prospection par voie électronique. Il s'agit dans une certaine mesure de pérenniser la « boîte à spam » ouverte par la CNIL durant l'été 2002. L'effectivité de cette mesure dépendra naturellement des moyens humains et techniques mis à sa disposition pour assurer, au quotidien, le suivi d'un tel dispositif.

Concernant les sanctions applicables en cas de violation du régime du consentement préalable issu de la directive du 12 juillet 2002, la Commission a, dans son avis relatif au projet de loi de transposition, recommandé que le décret d'application prévu par l'article introduisant en droit français le régime du consentement préalable instaure une amende — sanction prévue pour les contraventions de 5e classe — par adresse irrégulièrement collectée. Une telle disposition paraît, en effet, une sanction plus adaptée et plus dissuasive que les dispositions générales de l'article 226-18 du Code pénal.

En conclusion et dans l'attente d'un texte définitif, la CNIL ne peut que se féliciter de ce nouveau dispositif relatif aux communications électroniques non sollicitées qui pose le principe d'un consentement préalable dans les opérations de prospection opérées par voie électronique. Toutefois, les questions soulevées par les difficultés d'interprétation ou de mise en œuvre de ces nouvelles règles détermineront, dans une mesure non négligeable, l'effectivité de cette nouvelle réglementation.

C. Seule l'Europe a opté pour le consentement préalable *(opt-in)*

L'opération « boîte à spams » réalisée par la Commission a démontré, s'il en était nécessaire, le caractère international de cette forme de prospection.

Il a déjà été souligné que le phénomène avait moins pour origine l'Europe que d'autres régions du monde, surtout les États-Unis et la région Asie-Pacifique. La raison en est essentiellement la tradition « Informatique et libertés » de l'Europe qui a vu, outre les initiatives prises par la CNIL en France, dès le mois de février 2000 le Groupe dit « de l'article 29 » adopter un avis commun sur le sujet[1]. On notera également, ce qui avait conduit à son élaboration, que dès avant l'adoption de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[2] cinq États membres avaient opté pour le régime du consentement préalable en la matière (Allemagne, Autriche, Danemark, Finlande, Italie).

Mais le développement du phénomène du « spam » dans les autres régions du monde conduit également à l'adoption de réglementations qui se distinguent cependant de l'approche européenne et dont la mise en œuvre ne conduit pas encore à des résultats suffisants.

Ainsi, aux États-Unis, vingt-six États ont adopté une législation « anti-spam ». Ces différentes lois visent à réprimer le plus souvent l'usage abusif du bien d'autrui ou le piratage informatique des moyens des fournisseurs d'accès. Quelques législations consacrent l'existence d'un droit d'opposition, mais exprimé a *posteriori,* à recevoir des courriers électroniques ultérieurs. Le plus souvent ces législations condamnent la prospection par mél avec une adresse d'expéditeur fausse ou non

[1] Avis 1/2000 sur certains aspects du commerce électronique adopté le 3 février 2000.
[2] Voir point IV du présent chapitre.

valide. Ces dispositions ont fait naître un important contentieux qui a, dans certains cas, été l'occasion de sanctions très lourdes prononcées à l'encontre des « spammeurs ».

Au plan fédéral, plusieurs propositions de lois destinées à encadrer la pratique du *« spamming »* ont été déposées devant le Congrès depuis 1999 dont aucune n'a été à ce jour adoptée. L'association américaine des sociétés de marketing direct qui a toujours été hostile à un encadrement juridique du publipostage électronique a indiqué en octobre 2002 au gouvernement américain qu'elle y était désormais favorable à la condition que soit prévu le mécanisme du droit d'opposition a *posteriori.* Elle rejette en effet toute idée d'un régime de consentement préalable qui est largement préconisé par les associations américaines de consommateurs ou d'internautes.

Au Canada, une décision de justice de juillet 1999 condamne la pratique du « spam ».

En Extrême-Orient, le Japon a adopté une loi le 1er juillet 2001 qui encadre la pratique du « *spamming »* en posant le principe d'un droit d'opposition a *posteriori.* En Corée du Sud, la loi relative aux télécommunications et à la protection des informations adoptée fin 2002 encadre la pratique de la prospection par courrier électronique. Elle prévoit l'existence d'un droit d'opposition *a posteriori* et interdit la collecte des méls dans les espaces publics de l'internet. De plus, s'agissant de l'information relative à l'existence du droit d'opposition, il est prévu qu'elle soit rédigée, sur chaque message envoyé, en coréen et en anglais.

La question posée aujourd'hui au plan mondial est celle à la fois de la coopération entre autorités compétentes en la matière et du rapprochement des législations. Le souhait de la CNIL est qu'une initiative européenne soit prise en ce sens en 2003.

Chapitre 3

LA CYBERDÉMOCRATIE EN TEST

En France, comme dans toute démocratie vivante, il est rare qu'une année se passe sans échéance électorale significative. Mais 2002, année des élections présidentielles et législatives, est appelée à rester dans notre histoire politique une année électorale mémorable. Si la CNIL, autorité administrative indépendante, se tient totalement en dehors du débat politique, elle est de plus en plus sollicitée pour en régler ou arbitrer certains aspects. Cette intervention croissante qui peut être comparée à celle plus ancienne du Conseil supérieur de l'audiovisuel (CSA) tient à une réalité encore émergente : la communication politique et donc électorale passe désormais par les technologies de la communication électronique. Elle trouve plus fondamentalement sa source dans un principe juridique : l'opinion politique dont le vote est l'expression la plus formalisée est une donnée personnelle dès lors qu'elle fait l'objet d'un traitement informatique. Elle a pris dans les campagnes électorales de 2002 deux formes principales : le traitement de plaintes et l'avis sur des expérimentations de vote électronique.

I. LA CNIL ET LA CAMPAGNE

A. Un sondage politique par mél

Entre les deux tours des élections présidentielles de 2002, la société Impact Net a adressé à plusieurs milliers d'internautes un courrier électronique intitulé « Le dernier sondage avant le second tour des élections présidentielles 2002 ». Les internautes étaient invités à indiquer le nom du candidat pour lequel ils avaient voté au premier tour des élections ainsi que celui pour lequel ils avaient l'intention de voter au second tour. Il leur était assuré que leurs réponses seraient traitées anonymement.

Saisie par de nombreux internautes inquiets de recevoir ce sondage, la CNIL a effectué une mission de contrôle auprès de la société ayant procédé à son envoi, une société spécialisée dans la prospection commerciale par courrier électronique. Lors de cette mission de contrôle, les experts informaticiens de la CNIL ont pu trouver sur le serveur appartenant à cette société un fichier-texte comportant 19 056 réponses au sondage politique associées, dans la quasi-totalité des cas (entre 12 000 et 13 000), aux adresses électroniques des internautes.

Un fichier informatisé comportant les opinions politiques d'internautes identifiables par leur adresse électronique avait donc été mis en oeuvre par cette société.

La Commission, réunie en séance plénière le 9 juillet 2002, a décidé de dénoncer au Parquet les nombreux faits, imputables à cette société, susceptibles de constituer des infractions punies par le Code pénal.

En premier lieu, la Commission a estimé que les internautes sollicités avaient été faussement informés de ce que le sondage ne revêtait aucun caractère nominatif alors que leurs réponses étaient associées à leur adresse électronique, information indirectement nominative au sens de l'article 4 de la loi du 6 janvier 1978 (fait susceptible de constituer une collecte d'adresses électroniques opérée par un moyen frauduleux, déloyal ou illicite, infraction visée par l'article 226-18 du Code pénal).

La Commission n'a pu par ailleurs que constater que le consentement exprès des personnes concernées n'avait pas été recueilli préalablement à la mise en œuvre d'un traitement automatisé d'informations nominatives faisant apparaître leurs opinions politiques (fait susceptible de constituer l'infraction visée par l'article 226-19 du Code pénal).

La Commission a en outre considéré que cette société avait procédé à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi du 6 janvier 1978 (fait susceptible de constituer l'infraction visée par l'article 226-16 du Code pénal).

Enfin, la Commission a constaté que cette société avait indiqué avoir mis à disposition des adresses électroniques collectées à partir d'un de ses sites internet dont la déclaration, effectuée auprès de la Commission, précisait pourtant que les données ne seraient pas utilisées pour le compte de tiers (fait susceptible de constituer l'infraction visée par l'article 226-16 du Code pénal).

Le 20 janvier 2003, le parquet de Nanterre a classé sans suite ce dossier après avoir adressé un simple rappel à la loi à la société Impact Net.

B. Internet : nouvel outil des campagnes électorales

Internet est apparu, au cours de l'année 2002 marquée par les deux échéances électorales fondamentales, comme un outil commode permettant aux hommes politiques de communiquer avec leurs électeurs : il s'agit d'un moyen rapide, peu coûteux et moderne.

Tous les candidats à l'élection présidentielle ont en effet ouvert des sites internet permettant aux internautes de s'abonner à des listes de diffusion, de participer à des forums de discussion, d'adresser des messages électroniques aux candidats, etc.

L'usage d'internet dans les campagnes électorales a ainsi renouvelé les pratiques du « marketing politique » et la CNIL a souhaité rappeler les garanties prévues par la loi du 6 janvier 1978, applicables à toute opération de collecte, de traitement, de stockage et à toute utilisation des données personnelles concernant les internautes (leur adresse électronique, pour l'essentiel).

C'est dans cet esprit que la CNIL a adressé des courriers à tous les responsables de partis politiques et aux présidents des groupes parlementaires pour préciser les règles qui s'appliquent aux sites web de communication politique. Le souci de la CNIL était de rappeler aux partis, avant même le lancement des campagnes électorales, qu'il convient d'instaurer un climat de confiance sur internet en informant clairement les internautes de l'utilisation qui sera faite des données personnelles qu'ils communiquent à un parti ou à un candidat.

La CNIL a élaboré une fiche pratique proposant des mentions d'informations à faire figurer sur les sites des candidats. Elle a insisté sur la nécessité d'informer les internautes de la nature exacte du site visité (s'agit-il du site d'un parti politique, d'un comité de soutien à un candidat, d'un groupe de sympathisants ?) et sur le devenir des données qu'ils peuvent laisser sur ce site (leur adresse électronique sera-t-elle réutilisée à l'issue de la campagne ? Sont-ils clairement informés qu'ils peuvent s'opposer à cette réutilisation ? Leurs coordonnées seront-elles cédées au parti de rattachement du candidat ?).

Cette démarche, en amont, effectuée par la CNIL a permis aux sites mis en œuvre par des candidats de se conformer aux dispositions de la loi du 6 janvier 1978. Les mentions d'informations proposées par la CNIL ont été largement reproduites sur les sites des divers candidats aux élections et la CNIL a reçu très peu de plaintes.

Seules quelques plaintes émanant de particuliers ayant reçu des messages électroniques non sollicités de candidats aux élections lui ont en effet été adressées. La Commission a, dans ces cas, demandé aux émetteurs de ces messages de radier les plaignants de leurs fichiers.

II. LE VOTE ELECTRONIQUE

Face au désintérêt des citoyens pour la chose publique, diverses réflexions ont été engagées pour tenter de trouver des moyens afin d'endiguer, notamment, une abstention grandissante lors des divers scrutins.

La loi du 27 février 2002 relative à la démocratie de proximité a donné une première traduction législative à un mouvement entamé il y a plusieurs années. L'objectif était d'accentuer la participation des habitants à la vie des communes notamment par la création des conseils de quartier. D'autres initiatives visaient à

surfer sur la vague de l'internet afin d'utiliser ce dernier pour permettre une expression directe du citoyen depuis son domicile, une cyberdémocratie en quelque sorte.

Cette cyberdémocratie utiliserait en particulier le vote électronique et plus précisément le vote électronique à distance, par internet (le vote électronique sur place étant aussi envisagé mais pour d'autres raisons, plus pratiques en particulier quant au dépouillement) tant pour les élections politiques mais aussi des consultations diverses des habitants. Les propositions de lois se multiplient dans le sens d'une autorisation du vote par internet.

L'utilisation d'un vote électronique en matière d'élections implique une véritable réflexion au regard des enjeux soulevés si tant est qu'elle puisse amorcer un renouveau démocratique. Elle a de surcroît des implications potentielles en matière de protection des données personnelles.

La CNIL a pour mission de protéger la vie privée et les libertés individuelles en matière de traitement informatique de données nominatives (articles 4 à 6 de la loi du 6 janvier 1978). Son champ de compétences s'étend logiquement au vote électronique dès qu'il est procédé à un enregistrement de données personnelles. Préalablement à sa mise en œuvre, tout projet de vote électronique (sur place ou à distance) doit faire l'objet de formalités (demande d'avis ou déclaration) auprès de la CNIL. La Commission a d'ores et déjà été amenée à se prononcer sur différents projets.

Quels sont les éléments fondamentaux relatifs à la protection des données personnelles mis en jeu dans le cadre d'un vote électronique ?

Le vote électronique concerne à plusieurs titres la loi « Informatique et libertés » sur laquelle la CNIL a fondé sa démarche pour se prononcer sur les projets qui lui ont été soumis. Il ressort, de ces premières réflexions, plusieurs garanties nécessaires au respect de la protection des données personnelles en matière de vote électronique.

A. Le vote électronique au regard des principes fondamentaux de la loi « Informatique et libertés »

Le vote électronique constitue une opportunité pratique pour accélérer ou faciliter le vote lors d'élections politiques ou professionnelles. Il n'en doit pas moins respecter les principes fixés par la loi informatique et libertés. La CNIL a reçu pour mission de veiller à ce respect, ce qu'elle s'est efforcée de faire d'ores et déjà dans quelques décisions.

1. LES PRINCIPES JURIDIQUES DE LA LOI « INFORMATIQUE ET LIBERTÉS » APPLICABLES AU VOTE ÉLECTRONIQUE

Les principes définis par la loi « Informatique et libertés » (finalité, pertinence des données, sécurité, information des personnes) trouvent évidemment à s'appliquer aux expérimentations de vote électronique.

Parmi ces principes, deux d'enfre eux prennent une place importante en matière de vote électronique : le principe de finalité ainsi que le principe de sécurité.

a) La déclinaison du principe de finalité en matière de vote électronique

Le principe de finalité signifie que les informations nominatives recueillies et traitées doivent être pertinentes et adéquates par rapport à la finalité du traitement projeté et que leur durée de conservation doit être limitée en fonction de cette finalité.

En matière de vote électronique, la finalité est l'organisation d'une opération électorale. Cette dernière se caractérise au regard de l'article 3 de la Constitution par le fait que le vote est secret *(« universel, égal et secret »).* Le Code électoral rapelle également cette exigence en son article L. 59.

La finalité du traitement implique donc au moins pour les élections relevant du Code électoral le respect du caractère secret du vote ce qui signifie au plan de la protection des données personnelles qu'il ne doit pas y avoir de lien entre l'identité d'un électeur et l'expression de son vote. Le tribunal administratif de Lille dans un jugement du 23 juillet 1996, puis la cour administrative d'appel de Nancy (4 juin 1998) ont considéré, dans une même affaire, que l'utilisation de bulletins de vote comportant un code barre permettant l'identification du numéro du votant sur la liste d'émargement ainsi que le code barre de la liste pour laquelle le votant exprimait son choix conduisait à rompre l'anonymat et le secret du vote[1]. La transposition — électronique — d'un système similaire conduirait à une conséquence identique.

En matière de vote électronique sur place, la Commission a autorisé dans une délibération[2] du 14 mars 2002 le recours à un système d'identification des électeurs par une carte à microprocesseur comportant leurs empreintes digitales. Ces empreintes étaient enregistrées uniquement sur la carte sans constitution d'une base générale. Elles permettaient à l'ordinateur de vérifier l'enregistrement de l'électeur sur la liste électorale l'autorisant ensuite à voter sur un écran tactile d'ordinateur. Il n'y avait pas de lien entre la liste électorale et les bulletins de vote virtuels enregistrés sur un autre serveur.

b) Le principe de sécurité des données nominatives

Ce principe signifie que le responsable du traitement est astreint à une obligation de sécurité : il doit prendre toutes précautions utiles pour garantir la confidentialité des données, éviter leur divulgation et empêcher leur déformation.

[1] Saisi d'un recours en cassation, le Conseil d'Etat ne s'est pas encore prononcé.

[2] Délibération n° 02-015 du 14 mars 2002 concernant l'expérimentation d'un dispositif de vote électro nique reposant sur l'utilisation de cartes à microprocesseur comportant les empreintes digitales des élec teurs. Cette carte leur permettait de s'identifier, l'ordinateur vérifiant si l'électeur figure bien dans la liste électorale. Dans ce cas, il délivrait un certificat de vote qui était enregistré sur la carte. Une fois dans l'iso loir, l'électeur introduisait cette carte dans un deuxième ordinateur où il exprimait son vote par choix sur un écran tactile. Une fois validé le vote était transmis sous forme cryptée à un serveur centralisant les votes.

En matière de vote électronique, cela implique que les données personnelles soient protégées afin d'éviter toute fraude ou piratage, toute usurpation d'identité et garantir la prise en compte effective du vote.

Le principe de sécurité peut aussi être décliné sur le plan de la sincérité des opérations électorales qui doit être assurée par la surveillance effective du scrutin et le contrôle des opérations par des représentants du corps électoral, conformément aux articles L. 63, 65 et 67 du Code électoral.

Cela s'entend à la fois durant le vote mais s'étend évidemment au dépouillement. La Cour de Cassation a ainsi cassé, dans un arrêt du 20 octobre 1999, pour non-conformité avec les principes généraux du droit électoral, un jugement du tribunal d'instance de Paris au sujet d'un accord préélectoral prévoyant le recours à un vote par téléphone pour les élections des délégués du personnel et des membres du comité d'entreprise d'Aéroports de Paris. La Cour décide que même si les modalités d'organisation et le déroulement des opérations électorales font l'objet d'un accord entre le chef d'entreprise et les organisations syndicales intéressées, *« cet accord doit respecter les principes généraux du droit électoral »* articles L. 65, L. 67 et R. *57* du Code électoral selon la Cour). La Cour estime que la clôture du scrutin n'était pas publiquement constatée par le président du bureau de vote et que les opérations électorales (dépouillement en particulier) échappaient au contrôle des électeurs et des délégués de listes.

Il y a donc une conjonction des principes issus de la loi « Informatique et libertés » et des principes généraux du droit électoral.

L'utilisation du vote électronique implique de prendre en compte d'autres principes juridiques, indirectement liés à la protection des données mais qui ne peuvent être écartés tels le caractère personnel du vote et le principe d'égalité entre électeurs.

Tels sont les principes essentiels de la loi « Informatique et libertés » qui trouvent plus particulièrement à s'appliquer lorsque que la CNIL est saisie d'expérimentations de vote électronique. Elle a déjà rendu à cet égard, un certain nombre d'avis en particulier sur le vote par internet.

2. LA POSITION DE LA CNIL SUR LES EXPÉRIMENTATIONS DE VOTE ÉLECTRONIQUE

Si la Commission n'a pu examiner les expériences de Brest, Voisins-le-Bretonneux, de l'Ordre des avocats de Paris (absence de déclaration pour la première et pour la troisième, déclaration tardive pour la seconde), elle s'est prononcée en 2002 à trois reprises sur des expérimentations de vote électronique.

La ville de Vandœuvre-lès-Nancy a souhaité tester un système de vote par internet, parallèlement au vote traditionnel, à l'occasion de l'élection présidentielle d'avril-mai 2002[1]. La Commission a rendu un avis négatif sur ce projet aux motifs

[1] Délibération n° 02-022 du 2 avril 2002.

que le dispositif projeté ne garantissait pas l'identification certaine de l'électeur (envoi du code confidentiel par simple courrier à un domicile où il peut être récupéré par une tierce personne du foyer), l'anonymat du vote d'un bout à l'autre de l'opération technique (en plus d'associer expression du vote et identité de l'électeur) et le contrôle des opérations électorales (l'organisation matérielle du vote dépendait de dispositifs techniques situés à New York, échappant ainsi à tout contrôle effectif des autorités nationales compétentes).

La Commission a appliqué en l'espèce les principes de finalité et de sécurité ainsi que des principes généraux du droit électoral. Après plusieurs modifications techniques, l'expérimentation a pu avoir lieu sous forme d'un vote électronique sur place.

Plus récemment, la Commission a accepté une expérimentation de vote par internet à l'occasion des élections de membres de conseils de quartier à Issy-les-Moulineaux (délibération n° 02-090 du 28 novembre 2002). La Commission a estimé qu'en l'absence d'un cadre juridique[1], le recours à ce mode de consultation des habitants pouvait être admis compte tenu de son caractère expérimental et limité. Pour les élections aux conseils de quartier il n'y a ni texte prévoyant le principe d'une élection (mais seulement d'une désignation) ni jurisprudence. Il était donc difficile à la Commission de se substituer tant au législateur qu'au juge. C'était aussi une occasion d'autoriser pour la première fois, pour un enjeu limité, la possibilité d'un vote par internet, donc de faire un test dont le bilan est d'ailleurs intéressant.

S'agissant d'élections dans d'autres domaines, le vote par internet est plus utilisé même s'il ne fait guère l'objet de plus d'encadrement juridique.

La loi sur les nouvelles régulations économiques du 15 mai 2001 ajoute cependant un article L. 225-107 au Code de commerce prévoyant la possibilité pour les actionnaires de participer à une assemblée générale et d'y voter, notamment par internet.

En revanche, s'agissant des élections prud'homales, où le vote par correspondance est admis par le Code du travail, la Commission a rendu un avis défavorable[2] sur l'expérimentation projetée à Issy-les-Moulineaux. Elle a estimé que les modalités de fonctionnement du dispositif décrites dans la demande d'avis relatives à la coexistence sur un même serveur de l'identité de l'électeur et de son bulletin de vote ne lui donnaient pas l'assurance que le procédé garantissait effectivement le secret du suffrage et empêchait les scrutateurs ou les administrateurs de connaître l'expression du vote des électeurs avant la fin du scrutin. La coexistence sur un même serveur de l'identité des électeurs et des bulletins virtuels ne paraissait pas équivalente au système de la double enveloppe existant en matière de vote par correspondance.

[1] L'article 1er de la loi du 27 février 2002 relative à la démocratie de proximité prévoit qu'il appartient au conseil municipal de décider librement de la composition et des modalités de fonctionnement des conseils de quartier, en particulier de la désignation des membres de ces instances (une élection n'est pas nécessaire).

[2] Délibération n° 02-091 du 28 novembre 2002.

La doctrine de la Commission est certainement appelée à évoluer dès l'instant où les principes généraux du droit électoral et les règles en matière de protection des données personnelles seront respectés. Ces principes trouvent leur déclinaison pratique dans l'adoption d'un certain nombre de garanties minimales que la Commission souhaite voir respecter lors de la mise en œuvre des premières expérimentations.

B. Les garanties minimales à respecter dans le cadre des expérimentations de vote électronique

Ces garanties concernent d'une part la préparation des opérations électorales et du déroulement du vote et d'autre part le dépouillement des votes et le contrôle des opérations électorales.

1. LA PRÉPARATION DES OPERATIONS ELECTORALES ET DU DÉROULEMENT DU VOTE

La délivrance sous une forme confidentielle des identifiants et des codes d'accès au dispositif de vote constitue une première garantie essentielle. La nécessaire absence de lien entre les données nominatives des électeurs et leur bulletin de vote est un autre préalable indispensable.

a) La délivrance des identifiants et codes confidentiels

Si le vote électronique est subordonné à la saisie préalable d'un identifiant et d'un code d'accès au serveur de vote, l'attribution de ces codes doit être faite de façon sécurisée (génération aléatoire du code confidentiel) et leur délivrance aux électeurs doit également être totalement sûre.

Les codes doivent être placés sous enveloppe selon un système fiable (ex. : celui des codes de cartes bancaires) et imprimés selon un système sécurisé sans que le fichier comportant à la fois l'identité des électeurs et leurs codes personnels ne soit en clair. Ils doivent être délivrés personnellement à l'électeur (puisqu'il n'y aura pas de contrôle possible de la personne votant au moment du vote comme dans un scrutin classique où l'identité est contrôlée à l'entrée du bureau de vote). L'envoi par simple courrier de l'identifiant et du code personnel ne sont pas de nature à garantir cette sécurité. L'envoi par recommandé avec accusé de réception permet d'avoir un commencement de preuve en cas de contestation. Le certificat électronique est certainement une solution plus moderne et plus adaptée.

À cela s'ajoute la question de la sécurité dans l'utilisation du code confidentiel et de l'identifiant. Ceux-ci peuvent, en effet, être utilisés par une autre personne que celle à qui ont été délivrés ces éléments. Il est fondamental que l'on puisse s'assurer tant de l'identité du votant que du fait qu'il n'y a pas usurpation d'identité. La biométrie peut être une solution pour un vote électronique sur place mais nettement plus complexe à mettre en œuvre pour un vote électronique à distance.

b) L'absence de lien entre les données nominatives des électeurs et le bulletin de vote

Il est fondamental que le bulletin de vote virtuel soit séparé de l'identifiant et du code confidentiel et ne puisse en être rapproché. Il doit se trouver dans une urne virtuelle différente du serveur contenant les identifiants et les codes personnels c'est-à-dire les données personnelles du votant.

Il convient également que les clés, codes ou mots de passe divers permettant d'accéder au système en cours de vote ne conduisent pas à connaître de résultats partiels mais seulement l'état de la participation. Leur délivrance au président du bureau de vote et au scrutateur doit être également sécurisée.

c) Le cryptage des bulletins de vote

En matière de vote à distance, il est important pour des questions de sécurité informatique et afin de garantir la prise en compte de tous les votes que les bulletins de vote soient cryptés et ce dès le départ du terminal de vote.

Le chiffrement du vote doit être permanent d'un bout à l'autre de l'opération technique. Il ne doit pas comporter de passages « en clair » au cours des différentes phases de traitement.

S'agissant de l'expérience de Mérignac, le vote était transmis sous forme chiffrée avec un décryptage à l'issue du scrutin, sous le contrôle du président du bureau et des assesseurs. Le système prévu à Vandceuvre-lès-Nancy était différent et comportait un passage « en clair » avant l'enregistrement sur le serveur de vote.

2. LE DEPOUILLEMENT DES VOTES ET LE CONTROLE DES OPÉRATIONS ÉLECTORALES

Ces garanties doivent permettre un contrôle effectif des scrutateurs durant le vote et le dépouillement des bulletins.

a) Le contrôle des représentants du corps électoral (scrutateurs/assesseurs) durant le vote et le dépouillement

Celui-ci est déterminant dans une élection classique. Ces représentants participent au dépouillement et constatent physiquement le bon déroulement des opérations, en particulier la régularité du dépôt des bulletins de vote et de l'émargement.

Un système informatique ne peut s'affranchir de cette dimension. Le fait de confier à des prestataires privés la gestion et le contrôle des opérations électorales jusqu'alors assurés directement par des représentants du corps électoral soulève d'ailleurs une question de principe.

Le contrôle effectif des opérations électorales doit pouvoir se faire par des scrutateurs qui doivent avoir tous moyens de contrôler le bon déroulement informatique du scrutin. Cela signifie qu'ils doivent disposer de la documentation nécessaire

sur le système informatique, qu'ils doivent avoir été formés à son fonctionnement, informés des mesures des enjeux en matière de protection des données et des mesures prises à cet égard, du moyen de contrôler les opérations. Sinon comment dès lors s'assurer que son bulletin de vote a bien été pris en compte ? Ou que l'anonymat du vote est bien respecté ? En particulier, qu'il n'y ait pas de lien entre l'identité du votant et son bulletin virtuel.

Les scrutateurs/assesseurs garantissent aujourd'hui par leur présence la sincérité des opérations électorales, il est important de retrouver un système similaire.

En matière de dépouillement, le gain de temps du vote électronique est un avantage certain. Il ne doit cependant rien retirer à la nécessaire transparence de ce dépouillement.

b) Le dépouillement des votes

Le dépouillement des votes repose souvent sur un système de clé privée c'est-à-dire de codes à introduire dans le dispositif pour permettre le dépouillement (la clé est souvent divisée en plusieurs morceaux qui doivent être réunis pour déclencher les opérations). Le choix des personnes doit s'opérer selon une procédure objective et transparente. Les clés privées doivent en toute hypothèse être particulièrement bien gérées (génération des clés, qui les détient...).

Par ailleurs, il est important que l'électeur puisse s'assurer que son bulletin a bien été pris en compte dans le vote et lors du dépouillement. Comment garantir cela à l'électeur ? Comment garantir qu'il n'y a pas eu falsification ? Par des experts indépendants, des tests ?

c) La possibilité d'un contrôle *a posteriori*

Un huissier, par exemple, doit pouvoir contrôler le bon déroulement des opérations et du dépouillement y compris sur les aspects techniques et pas seulement dresser un constat des noms des élus qu'on lui communique. Il doit donc bien connaître aussi le système. Les difficultés rencontrées par les électeurs pour voter par internet doivent pouvoir être consignées.

Les conditions doivent être réunies, enfin, pour que le juge des élections puisse aisément entreprendre des contrôles si nécessaire sur le déroulement des opérations de vote ou le dépouillement. La conception du système doit donc être réalisée afin de lui permettre d'exercer son contrôle sans problème en particulier s'agissant de l'accès et de la localisation du système informatique.

Les premiers avis de la CNIL permettent donc de dresser un premier éventail de garanties minimales à respecter pour une expérimentation de vote électronique. La confiance dans de tels systèmes ne peut se décréter. Les arguments commerciaux ou politiques n'empêcheront pas une méfiance légitime des électeurs vis-à-vis de ces systèmes de vote et toutes les conditions doivent au contraire être réunies pour établir cette confiance. Les citoyens ont déjà des hésitations concernant le paiement des achats sur internet et exigent de hautes sécurités, il ne peut en être autrement d'un vote par internet compte tenu des enjeux. Cette confiance ne viendra que lorsque les

garanties minimales de sécurité pourront être apportées de façon claire et certaine. Les procédures classiques de vote n'empêchent pas la fraude mais celle-ci reste marginale et est souvent facilement décelable en raison précisément de systèmes de vote simples, clairs et aisément contrôlables.

Des expérimentations de vote électronique peuvent être menées, mais elles ne sauraient avoir lieu que si les modalités de leur mise en œuvre sont suffisamment sécurisées. Le vote électronique constitue certainement une opportunité intéressante pour un certain nombre de scrutins mais, sous l'angle de la protection des données personnelles, il exige l'adoption de fortes garanties en terme de sécurité et de protection du caractère anonyme du vote. Il est fondamental que ces éléments soient pris en compte si l'on veut créer le climat de confiance nécessaire à l'adhésion des citoyens.

Chapitre 4

INTERNET ET CONFIDENTIALITÉ

« *Au village sans prétention, j'ai mauvaise réputation* »
Georges Brassens.

Au village planétaire de l'internef *non* seulement notre réputation peut être rapidement entachée par l'efficacité des moteurs de recherche qui mettent à jour le moindre de nos écarts avec la justice ou l'administration, mais notre numéro de carte bancaire semble circuler allègrement, engendrant parfois des dépenses somptuaires dans d'exotiques villégiatures où jamais nous ne mîmes pied. La CNIL pour sa part milite pour qu'internet et confidentialité fassent bon ménage, afin de préserver des intérêts qui sont autant moraux que matériels. Mais en dernier ressort la protection de ces intérêts ne peut être assurée que par un juge : dès lors se pose la question de savoir si c'est le juge français ou le juge du pays où est établi le responsable du site internet, à supposer qu'il soit identifiable, qui pourra le faire. A moins que l'on ne s'en remette à des grands opérateurs privés pour assurer la confidentialité des données... qui leur sont confiées.

I. LA PRESERVATION DE L'ANONYMAT

A. Les suites de la recommandation sur l'anonymisation des décisions de justice

La CNIL a adopté, le 29 novembre 2001, une recommandation préconisant l'anonymisation des décisions de justice librement accessibles sur internet : le nom et l'adresse des parties et des témoins doivent être occultés des jugements et arrêts accessibles sur internet dès lors que le site est en accès libre[1].

[1] *Cf.* 22e rapport d'activité 2001, p. 73.

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

En 2002, plusieurs personnes ont saisi la CNIL après avoir constaté qu'en interrogeant un moteur de recherche sur leur nom, n'importe qui pouvait accéder à des décisions de justice ou des décisions disciplinaires prononcées contre elles.

Les trois exemples suivants illustrent des cas où quiconque — un voisin, un membre de la famille, l'employeur — équipé d'internet peut, depuis son domicile, prendre connaissance, même par hasard, d'une condamnation ou d'une sanction disciplinaire frappant une personne.

1. LA DIFFUSION DES DÉCISIONS DE JUSTICE FRANÇAISES SUR LE SITE LÉGIFRANCE

M. T. appelle l'attention de la CNIL sur la diffusion, par le site www.legifrance.gouv.fr, d'un arrêt rendu par une juridiction administrative comportant son identité. On pouvait y apprendre que M. T. s'était vu refuser l'agrément pour être gérant de tutelle. La décision comportait en outre son adresse personnelle.

Cet arrêt fait partie des 428 000 décisions de justice qui étaient précédemment diffusées, en accès payant, sur le site Jurifrance. Depuis septembre 2002, ces décisions sont accessibles gratuitement sur le site Légifrance, et comme on le verra ci-dessous plus en détail, le gouvernement s'est engagé à les rendre plus anonymes.

Un délai de deux ans étant nécessaire à l'anonymisation globale de ce stock, certaines décisions demeurent accessibles sous une forme nominative. Comme M. T., les personnes concernées par ces décisions disposent de la faculté de demander leur anonymisation au cas par cas.

Le secrétariat général du Gouvernement, responsable du site internet (Légifrance), saisi par la CNIL, a immédiatement procédé à l'anonymisation de l'arrêt concernant M. T.

2. LA DIFFUSION SUR INTERNET DES DECISIONS DU TRIBUNAL ADMINISTRATIF DE L'ORGANISATION INTERNATIONALE DU TRAVAIL (OIT)

M^{me} F. proteste auprès de la CNIL contre la diffusion d'un jugement rendu par le tribunal administratif de l'OIT la concernant sur le site du tribunal. On pouvait y apprendre que M^{me} F., employée d'une organisation internationale, malade depuis 1992, bénéficie d'une pension d'invalidité et qu'elle rencontre des difficultés juridiques avec son employeur.

Bien que la loi française ne s'applique pas aux juridictions internationales, la CNIL a décidé de saisir le tribunal administratif de l'OIT, afin de lui faire part de sa recommandation du 29 novembre 2001 préconisant l'anonymisation des décisions de justice librement accessibles sur internet.

Le tribunal administratif de l'OIT a procédé à l'anonymisation du jugement concernant M^{me} F. et a en outre pris l'engagement d'anonymiser systématiquement, à l'avenir, les jugements mis en ligne sur le site internet de l'OIT.

3. LA DIFFUSION SUR INTERNET DU BULLETIN OFFICIEL DU MINISTÈRE DE L'ÉDUCATION NATIONALE

La CNIL avait déjà été alertée, en 2001, sur la mise en ligne, sur internet, par le ministère de la Jeunesse et des Sports du Bulletin officiel du ministère (le BOJS) qui comportait, notamment, la liste des personnes ayant été frappées d'une mesure d'interdiction d'exercer des fonctions d'encadrement dans les centres de vacances et de loisirs (« cadres interdits »).

Saisi par la commission sur ce point, le ministère de la Jeunesse et des Sports avait décidé de suspendre cette diffusion dans l'attente de la mise en place d'un système permettant aux seules personnes habilitées d'y avoir accès[1].

En 2002, l'attention de la CNIL a été appelée par deux personnes à propos de la diffusion sur le site internet du ministère de la Jeunesse, de l'Education nationale et de la Recherche, des décisions disciplinaires des établissements publics d'enseignement supérieur parues au Bulletin officiel de ce ministère. Ces décisions dressent la liste des personnes ayant fait l'objet d'une mesure d'exclusion définitive ou temporaire d'un établissement public d'enseignement, ou d'une mesure d'interdiction de passer un examen, et précisent le motif de la sanction.

Tel est le cas, par exemple, de M. P. frappé d'une interdiction d'un an avec sursis de passer le baccalauréat pour cause de tricherie.

S'il est légitime que ces décisions soient accessibles aux administrations (universités, centres d'examen, établissements d'enseignement, etc.) chargées de les appliquer, rien ne justifie en revanche que n'importe qui puisse en prendre connaissance. Or, tel est le cas en l'espèce.

Ainsi, et dans la mesure où la mise à disposition du public, sur internet, de telles décisions est de nature à soulever des difficultés au regard des règles relatives à la protection des données des personnes concernées, et notamment des articles 26, 29 et 30 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la CNIL a demandé au ministère la Jeunesse, de l'Education nationale et de la Recherche de prendre des mesures afin que le site www.education.gouv.fr ne permette plus un accès libre aux décisions disciplinaires des établissements publics d'enseignement supérieur parues au Bulletin officiel. L'élaboration d'une solution est en cours en collaboration avec les services de ce ministère.

[1] *Cf. 22^{e}* rapport d'activité 2001, p. 89.

D'une manière plus générale, la CNIL a décidé d'entamer une réflexion avec l'ensemble des ministères concernant la diffusion des bulletins officiels sur internet. Il convient en effet d'examiner celles des décisions dont la publication sur internet, en accès libre, est de nature à porter atteinte aux droits et libertés des personnes concernées.

B. Le site internet Légifrance

Le Secrétariat général du gouvernement a procédé à différentes modifications de son site web www.legifrance.gouv.fr et a saisi en conséquence, pour avis, la CNIL d'une demande d'avis modificative au mois de juillet.

Cette refonte fait suite à l'adoption du décret du 7 août 2002 relatif au service public de la diffusion du droit par l'internet, qui substitue au régime payant de diffusion en ligne de certaines données juridiques (« Jurifrance ») un portail unique qui assure désormais cette diffusion gratuitement. Le site Légifrance constitue désormais le portail unique d'accès au droit fournissant, gratuitement, l'intégralité de ces textes, ainsi que les arrêts et jugements sélectionnés.

Le gouvernement, conformément à la recommandation de la CNIL du 29 novembre 2001 sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence et comme il s'y était engagé, a procédé à l'anonymisation des arrêts et jugements mis en ligne sur le site Légifrance (cf. 22e rapport d'activité).

Dans cette recommandation, fruit d'une concertation approfondie avec l'ensemble des acteurs concernés, la commission a notamment préconisé que les éditeurs de bases de données recensant des décisions de justice librement accessibles sur des sites internet s'abstiennent, dans le souci du respect de la vie privée des personnes physiques concernées et de l'indispensable « droit à l'oubli », d'y faire figurer le nom et l'adresse des parties au procès ou des témoins.

Le secrétariat général du gouvernement a décidé d'intégrer les recommandations de la CNIL à l'occasion de la refonte du service public des bases de données juridiques. Ainsi, les décisions qui seront diffusées à l'avenir sur le site Légifrance seront-elles préalablement anonymisées.

Le gouvernement a également pris l'engagement de procéder, sur une période qui ne devrait pas dépasser deux ans et selon un ordre de priorité par matière déterminée par chaque juridiction, à l'anonymisation des décisions déjà mises à la disposition du public sur le site Jurifrance.

Néanmoins, des mesures techniques de protection des données sont prévues pour empêcher que le contenu des bases de données de jurisprudence ne soit indexé par les moteurs de recherche actuellement disponibles sur internet et limiter les procédés permettant « l'aspiration » du site ; de surcroît, le moteur de recherche du site Légifrance n'offre pas la possibilité d'effectuer une recherche de documents à partir du champ « nom des parties ».

Il doit également être rappelé que les personnes concernées par ces décisions peuvent demander leur anonymisation au cas par cas, comme l'exemple évoqué plus haut le montre.

Par ailleurs, conformément aux souhaits de la Commission, le choix a également été fait de ne pas diffuser en ligne certaines mesures nominatives publiées au *Journal officiel.* Il en est ainsi des textes relatifs à la nationalité, à l'état civil, ainsi que certaines décisions administratives ou juridictionnelles défavorables dont la publication constitue parfois une sanction accessoire.

La Commission avait en effet demandé que soient exclus de la diffusion par minitel et internet les décrets portant naturalisation, réintégration, mention d'enfant mineur bénéficiant de l'effet collectif attaché à l'acquisition de la nationalité française par les parents et francisation de noms et prénoms. En outre, et à la suite d'une plainte dont la Commission avait été saisie, le gouvernement s'était engagé à exclure de la version électronique du *Journal officiel* les décrets portant changement de nom.

La demande d'avis modificative soumise à la commission prévoit également l'exclusion de la version électronique du *Journal officiel* de nouvelles catégories de textes. Il s'agit des décrets et arrêtés portant exclusion de droit de la Légion d'honneur, des contrôles de la médaille militaire et de l'ordre national du Mérite, des arrêts de la cour de discipline budgétaire et financière, des décisions de sanction du Conseil de prévention et de lutte contre le dopage, des avis de la COB relatifs à des décisions de sanction.

La Commission a estimé que les précautions ainsi prises par le Gouvernement étaient de nature à préserver les droits et libertés des personnes concernées et a en conséquence émis un avis favorable au projet d'arrêté du Premier ministre portant modification du site.

II. LA CONSERVATION DU NUMERO DE CARTE BANCAIRE

La CNIL intervient régulièrement pour améliorer la sécurité liée à l'utilisation des coordonnées bancaires des consommateurs[1] :

— elle a ainsi été à l'origine des recommandations visant à la suppression du numéro complet de la carte figurant sur les facturettes des commerçants ;

— elle s'est penchée en 2000 sur le risque de captation du numéro lorsqu'il transite sur internet. Son étude réalisée sur cent sites de commerce électronique a révélé à l'époque que pour 96 % d'entre eux, l'envoi de données bancaires est associé à une technique de chiffrement ;

— elle s'intéresse maintenant à la question de la conservation du numéro par les commerçants.

[1] « Crédit et paiement : la sécurité à tout prix ? — La sécurisation des cartes bancaires », 21e rapport d'activité2000, p. 165.

A. L'inquiétude des consommateurs

Les services de la CNIL ont été saisis au cours de l'année 2002 d'un nombre croissant de plaintes de la part de consommateurs ayant pour objet la conservation et l'utilisation de leur numéro de carte bancaire par les commerçants spécialisés dans la vente à distance, qu'il s'agisse de vente par téléphone, courrier postal ou sur internet.

Il s'agit par exemple des clients de certains hôtels qui, en faisant une réservation par téléphone, s'aperçoivent que leurs informations bancaires ont été conservées depuis leur dernier passage dans l'hôtel. Il s'agit encore de débits effectués malencontreusement par certains fournisseurs d'accès internet auprès de leurs clients alors même que le compte était résilié mais que les informations bancaires contenues dans la base clients étaient toujours activées.

S'agissant plus spécifiquement des sites de commerce en ligne, l'attention de la commission a été appelée par les internautes sur trois points particuliers :

— Les conditions de confidentialité dans lesquelles les numéros de cartes bancaires sont conservés sur les serveurs des commerçants. De nombreux internautes s'interrogent en effet sur les conditions de sécurité appliquées aux bases de données comportant les numéros de carte bancaire.

— Les utilisations nouvelles faites de la carte bancaire. Le numéro de carte bancaire est en effet devenu un véritable « outil marketing » au service des commer çants qui l'utilisent pour la fourniture de services spécifiques et distincts du paiement du bien pour lequel le numéro de carte bancaire avait été communiqué par le consommateur. Il s'agit par exemple, sur internet, de la technique dite du « porte feuille électronique », c'est-à-dire la mémorisation automatique du numéro de carte bancaire dans un « compte client », afin que le consommateur n'ait plus à le ressaisir lors de ses éventuels futurs achats. Nul doute que de tels usages ont vocation à se mul tiplier dans l'avenir.

— La conservation sans durée précise par certaines entreprises des coor données bancaires de leurs clients.

B. Quels principes ?

La CNIL, soucieuse du respect de la confidentialité attachée aux données bancaires lors d'une opération de paiement, en particulier sur internet, souhaite donc préciser les règles permettant la mise en œuvre de pratiques nouvelles dans le respect des dispositions de la loi « Informatique et libertés ». La Commission entend ainsi porter sa réflexion sur les conditions de stockage des numéros de carte bancaire sur les bases de données des commerçants spécialisés dans la vente à distance. Elle a ainsi engagé une large concertation avec les principales fédérations professionnelles, associations de consommateurs et pouvoirs publics dans la perspective d'une recommandation qui devrait être adoptée dans le courant de l'année 2003.

Sur le plan juridique, la CNIL souhaite porter sa réflexion sur l'application de certains grands principes relatifs à la protection des données.

1. LA RECHERCHE D'UNE FINALITE DETERMINEE ET LEGITIME

La collecte et la conservation du numéro de carte bancaire dans un traitement automatisé d'informations nominatives doivent s'effectuer dans le respect des dispositions posées par l'article 5 de la convention n° 108 du Conseil de l'Europe, c'est-à-dire dans le respect de finalités déterminées et légitimes. Les données collectées doivent par ailleurs être pertinentes, adéquates et non excessives au regard de ces finalités et conservées pendant une durée proportionnée à ces finalités.

Si les entreprises se livrent très facilement à la collecte et au stockage des coordonnées bancaires de leurs clients, la détermination des finalités liées à cette collecte est très souvent inexistante. Il apparaît pourtant en pratique que les références d'une carte bancaire sont utilisées pour certaines finalités distinctes du paiement : portefeuille électronique, lutte contre la fraude, etc.

2. LA DUREE DE CONSERVATION DES NUMEROS DE CARTES BANCAIRES

La conservation du numéro de carte bancaire dans un traitement automatisé d'informations nominatives doit s'effectuer dans le respect des dispositions posées par l'article 5-e de la convention n° 108 du Conseil de l'Europe, c'est-à-dire pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles l'information est exigée.

Ainsi, lorsque le paiement est la finalité, la durée de conservation sera par exemple fixée en fonction des délais de réclamation liés à une opération par carte bancaire, argument avancé fréquemment par les déclarants pour justifier la conservation du numéro de carte bancaire du client. Sur ce chapitre, les dispositions de l'article L 132-6 du Code monétaire et financier prévoient que *« le délai légal pendant lequel le titulaire d'une carte de paiement ou de retrait a la possibilité de déposer une réclamation est fixé à soixante-dix jours à compter de la date de l'opération contestée. Il peut être prolongé contractuellement, sans pouvoir dépasser cent vingt jours à compter de l'opération contestée ».*

La Commission entend ainsi porter une attention particulière aux durées de conservation prévues par les responsables du traitement.

3. LA CONFIDENTIALITE DES DONNEES COLLECTEES

Tout responsable d'un traitement automatisé de données nominatives est tenu, en vertu de l'article 29 de la loi du 6 janvier 1978, de prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. Le responsable d'un fichier n'ayant pas respecté ces dispositions s'expose ainsi, en vertu de l'article 226-17 du Code pénal, à une peine d'emprisonnement de cinq ans ainsi qu'à une peine d'amende de 300 000 euros.

À cet égard, on peut s'interroger sur les conditions dans lesquelles la base de données sur laquelle le commerçant stocke les données bancaires est protégée tant vis-à-vis des accès du personnel de l'entreprise que vis-à-vis de tiers. Sur ce point, les services de la commission souhaitent faire le point sur les procédures internes définies par les entreprises.

On peut également s'interroger sur les conditions techniques dans lesquelles les dernières versions des navigateurs internet, comme Internet Explorer, permettent l'enregistrement systématique des mots de passe, qui, associés à un « cookie », autoriserait tout tiers utilisant l'ordinateur à avoir accès au « profil client » d'un site de commerce en ligne, et ainsi aux coordonnées bancaires de ce client, avec comme conséquence la réalisation d'achats frauduleux.

4. L'INFORMATION ET LE CONSENTEMENT PRÉALABLE *« OPT-IN »* DES PERSONNES FICHÉES

L'information préalable des personnes fichées est l'un des principes essentiels prévus par la loi Informatique et libertés. La directive du 24 octobre 1995, en imposant aux responsables de traitements d'informer les personnes fichées sur les finalités relatives à la collecte d'informations personnelles, offre ainsi un niveau d'information encore plus élevé.

Dès lors que les données relatives au numéro de carte bancaire sont utilisées pour une autre finalité que le traitement du paiement, le déclarant devrait, dans sa déclaration, préciser à la commission quelle est la finalité poursuivie par le traitement ainsi que la durée du stockage des données.

La mise en œuvre de traitements contenant le numéro de carte bancaire requiert ainsi une information claire et précise du client sur les finalités de la collecte.

Par ailleurs, la Commission serait encline à préconiser le recueil du consentement exprès de la part des personnes fichées, exprimé, par exemple, par l'existence d'une case à cocher, dès lors que leurs données bancaires sont utilisées pour d'autres finalités que le paiement.

Il est à noter que, sur la recommandation des services de la Commission, plusieurs grands acteurs de la vente en ligne ont d'ores et déjà retenu le principe de l'accord préalable *« opt-in »* du client pour la conservation de son numéro de carte bancaire.

III. LA DIMENSION INTERNATIONALE

Le développement mondial des communications grâce à internet, et ce aux fins les plus diverses, induit une multiplication des traitements de données à caractère international. Dans ce contexte, les internautes ont a *priori* peu de moyens de savoir dans quel pays le responsable du site sur lequel ils se connectent est établi, ni de quelle protection leur vie privée peut bénéficier dans ce nouveau contexte.

Cette problématique renvoie à la question dite de « détermination du droit national applicable » en droit international privé. La directive 95/46/CE traite de cette question en son article 4. L'interprétation des dispositions de cet article et leur application homogène aux sites internet dont les responsables sont établis soit dans un État membre de l'Union européenne, soit dans un pays tiers constituent un enjeu commun pour l'ensemble des États de l'Union. C'est pourquoi le groupe des autorités des États membres en charge de la protection des données réunies au sein du groupe dit de « l'article 29 » s'est attaché à examiner cette question en 2002, afin de fournir des lignes directrices communes aux responsables de sites et aux citoyens de l'Union européenne.

Par ailleurs, le développement commercial du service Passport offert par Microsoft au plan mondial depuis les États Unis a été l'occasion d'une application concrète de cette approche.

A. La question du droit national applicable

1. L'ARTICLE 4 DE LA DIRECTIVE 95/46

La directive de 1995 aborde, en son article 4, la question du droit national applicable aux opérations de traitements informatisés de données à caractère personnel. Cette question s'avère fort délicate et la CNIL, comme les autres autorités nationales de protection des données, est régulièrement invitée à conseiller particuliers et professionnels sur ce point. C'est ainsi à un moment fort opportun que le groupe de travail dit « de l'article 29 », lors de sa séance du 30 mai 2002, a adopté un document de travail traitant de ces questions de droit national applicable en matière de protection des données au traitement des données à caractère personnel sur internet *par* des sites web[1].

L'article 4 de la directive a deux objectifs principaux dont les conséquences vis-à-vis des sites internet sont les suivantes.

Un premier objectif consiste à éviter que, au sein de l'Union européenne, plusieurs législations nationales de transposition de la directive puissent s'appliquer à un même traitement. De tels conflits de lois (plusieurs lois nationales applicables au même traitement) n'ont en effet plus d'enjeux pratiques, la directive, dont c'est précisément l'objet, ayant instauré un niveau de protection équivalent dans tous les pays de l'Union européenne. Ainsi, lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire d'un État membre, seul le droit de cet État sera applicable à ce traitement. En revanche, si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il devra respecter, pour chacun de ses établissements, les obligations prévues par chacune de ces législations (article 4-1-a).

[1] Document de travail WP56 « Application internationale du droit de l'Union européenne en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'Union européenne », 30 mai 2002, 5035/01/EN/final, disponible sur internet.

En application de cette règle les traitements mis en œuvre dans le cadre de sites internet, quel que soit leur lieu de mise en œuvre, sont soumis à la loi de l'Etat membre dans lequel le responsable du site est établi.

Le second objectif consiste à protéger les utilisateurs alors que le responsable de traitement n'est pas établi dans l'Union. Cette préoccupation est spécifiquement relevée au considérant 20 de la directive : « *l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive* ». Afin d'atteindre cet objectif, l'article 4-1-c de la directive soumet les traitements de données effectués par un responsable de traitement établi dans un pays tiers à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés (sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté).

L'application de l'article 4 aux cas de collecte de données à caractère personnel sur internet, et plus précisément le rôle de cet article à l'égard de conflits de lois entre la loi nationale d'un État membre et celle d'un pays tiers, constitue un enjeu immédiat compte tenu du développement mondial du réseau des réseaux.

Cet enjeu peut être formulé de la façon suivante : un internaute européen se connectant à un site dont, le plus souvent, il ignore la localisation, peut-il prétendre à la protection assurée en Europe, ou bien faut-il accepter que la directive le laisse démuni ?

Autrement dit, les règles nationales du pays de résidence de l'utilisateur européen s'appliquent-elles à la collecte en ligne des données de celui-ci par un site web établi hors d'Europe, ou doit-on ne soumettre cette collecte qu'à la loi nationale de protection des données de ce pays tiers — étant observé que cette loi nationale n'existe peut-être pas, et que son niveau de protection sera forcément inférieur à celui de la directive ? Les réponses sont diverses et, selon l'option de politique juridique choisie, on interprétera différemment l'article 4 (c), et notamment le terme de « moyens ».

Cette question a fait l'objet de discussions approfondies au sein du groupe de l'article 29, au terme desquelles le groupe a adopté le document de travail précité.

2. L'INTERPRETATION DU GROUPE DIT DE « L'ARTICLE 29 »

Au préalable, le document du groupe relève que la détermination du droit national applicable n'est pas spécifique à la protection des données, ni à l'internet, ni à l'Union européenne, et fournit de nombreux exemples à cet égard[1]. En effet, il

[1] Ainsi, dans le secteur des compagnies aériennes, le règlement du Conseil intitulé « Code de conduite des SIR » (systèmes informatisés de réservation] s'applique aux systèmes informatisés de réservation proposés et/ou utilisés sur le territoire de la Communauté, indépendamment du statut ou de la nationalité du vendeur du système, ou de l'implantation de l'unité centrale de traitement des données. De même, aux Etats-Unis, le législateur et les juridictions appliquent des raisonnements similaires afin de soumettre des sites web étrangers aux réglementations locales : la loi américaine « *Children's Online Privacy Protection Act* » (COPPA) de 1998 s applique ainsi aux sites web étrangers qui collectent des informations personnelles des enfants établis sur le territoire des États-Unis. Enfin, en France, la célèbre affaire « Yahoo ! » montre également comment une juridiction française applique le droit pénal national pour interdire l'accès à des contenus nazis sur des serveurs internet étrangers. De nombreux autres exemples sont fournis par le document du groupe (pages 3 à 5).

s'agit d'une question générale de droit international qui se présente dans les situations en ligne et hors ligne, dans lesquelles un ou plusieurs éléments présents concernent plus d'un pays. Or l'on observe dans tous les cas mentionnés que le choix de l'application des règles nationales à des actes réalisés sur le territoire de pays tiers est communément fait, par le législateur comme par le juge, quand il s'agit de protéger des nationaux.

En tout état de cause, le document tient un premier élément pour acquis : les règles de la directive 95/46/CE s'appliquent au traitement de données à caractère personnel par le biais de « cookies », « JavaScripts », bannières et applications similaires, quand bien même le responsable de traitement serait établi dans un pays tiers. En effet, dans tous ces cas, le responsable de traitement, c'est-à-dire le responsable du site établi dans un pays tiers, a décidé d'utiliser l'ordinateur individuel de la personne à des fins de traitement, et plusieurs opérations techniques ont lieu sur cet ordinateur sans que la personne concernée ait un pouvoir de contrôle sur elles : l'applicabilité des règles européennes, en vertu de l'article 4-1-c, ne fait alors aucun doute.

En revanche, une autre discussion n'est pas spécifiquement abordée par le document : faut-il ou non considérer les règles de la directive comme applicables à la collecte en ligne par un formulaire de données à caractère personnel saisies par les utilisateurs, résidents européens, alors que le site web est établi hors de l'Union européenne ?

Certaines autorités européennes de protection des données, dont la CNIL, n'ont aucun doute sur la réponse à apporter à cette question : les règles européennes s'appliquent à la collecte de données traitées par un site web établi hors de l'Union européenne ou de l'Espace économique européen, alors que les données ont été saisies par l'utilisateur au moyen d'un formulaire électronique en Europe.

En effet, il est juste de considérer qu'un internaute européen qui communique volontairement des données le concernant à un site web non situé dans l'Union européenne se croit protégé par les règles en vigueur dans son propre pays, par exemple, en matière de loyauté de la collecte des données, et de transparence dans l'utilisation qui en sera faite. Accepter de communiquer avec un site hors Union européenne ne peut à l'évidence avoir pour conséquence de dépouiller l'internaute de ses droits : sinon ce serait entraver gravement le développement des échanges par internet au plan planétaire, et notamment le développement du commerce électronique.

Il convient cependant, sans aucun doute, d'adopter une attitude souple envers les conséquences pratiques de cette solution. À titre d'exemple, un souci de réalisme et de flexibilité pourrait conduire à envisager que le responsable de traitement établi dans un pays tiers soit exonéré de l'obligation de déclaration de ses traitements auprès des autorités de contrôle européennes. Cette déclaration serait d'autant moins nécessaire que le site internet est ouvert au public et permet à tout un chacun de prendre connaissance de l'identité du responsable de traitement et des données collectées sur le site.

Ainsi que l'indique le document de travail, le groupe dit « de l'article 29 » a l'intention de revenir sur ces questions, notamment à la lumière de l'expérience que les autorités nationales de protection des données acquerront à l'avenir.

B. Les services d'authentification en ligne : .Net Passport Microsoft et Liberty Alliance

Lors de sa réunion des 21 et 22 février 2002, la CNIL (qui avait consacré certains de ses travaux de 2001 à ces questions[1]) et ses homologues, réunis au sein du groupe dit « de l'article 29 », ont constaté qu'elles étaient saisies de nombreuses questions, voir de plaintes concernant le service Net Passport de Microsoft. Compte tenu du caractère international de ce nouveau service et de l'émergence d'initiatives concurrentes dans le domaine de l'authentification en ligne des internautes, notamment au sein d'une coopération entre plusieurs industriels sous l'appellation Liberty Alliance, les commissaires en charge de la protection des données dans l'Union européenne ont décidé de procéder à une démarche commune pour analyser ces projets. L'objectif de cette analyse était d'émettre des recommandations communes sous l'angle de la protection des données personnelles et, si nécessaire, d'établir un dialogue avec les entreprises impliquées afin que les traitements de données mis en œuvre dans le cadre de leurs services puissent être mis en conformité à la législation européenne et aux lois nationales de transposition.

Le groupe a publié deux documents de travail sur la question. Le premier, adopté le 2 juillet 2002, a déterminé les domaines de préoccupations communs sur lesquels le groupe souhaitait établir une concertation avec les acteurs concernés[2]. L'objectif de ce document consistait à constituer une base d'élaboration de recommandations ultérieures, et surtout, le service étant déjà en oeuvre, à obtenir certaines modifications du service. Net Passport offert par Microsoft. Le deuxième document a été adopté le 29 janvier 2003[3]. Il comporte une description détaillée des services concernés, établit une liste de recommandations pour leur mise en œuvre et prend note des engagements particuliers pris par Microsoft pour améliorer de manière substantielle les conditions de mise en oeuvre de Net Passport. Le texte intégral de ce document de travail est publié en annexe à ce rapport *[cf.* annexe 7).

Pour les autorités européennes, il ne fait pas de doute que la mise en oeuvre des services d'authentification, qui apportent des garanties quant à l'authentification des internautes (ne serait-ce que sous la forme d'une adresse de courrier électronique) aux tiers fournissant des services auxquels les internautes accéderaient, lorsqu'ils concernent des internautes résidant en Europe, sont soumis à la législation européenne de protection des données personnelles. Cette exigence découle directement des critères du droit national applicable dans le contexte de ces services d'authentification. Ainsi cette législation est applicable soit du fait de l'établissement des sociétés, en particulier Microsoft, qui mettent en œuvre le service en Europe (article 4-1-a de la directive 95/46/CE), soit du fait de l'établissement en Europe des organismes qui recourent à ces services à des fins d'authentification des internautes

[1] 22" rapport annuel 2001, chapitre 3 le marché de l'identité numérique, page 97 à 104.

[2] Document de travail WP 60 — « Premières orientations du groupe art. 29 — protection des données sur des services d'authentification en ligne », adopté le 2 juillet 2002, disponible sur internet à l'adresse suivante : http ://europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_fr.htm

[3] Document de travail sur les systèmes d'authentification en ligne WP 68, adopté le 29 janvier 2003, dispo nible sur internet.

(article 4-1-a), soit enfin du fait que des moyens de traitement des données sont localisés sur le territoire d'un État membre de l'Union européenne aux fins d'authentifica-tion des internautes par le service d'authentification (article 4-1-c). Il s'agit ici du terminal que l'internaute utilise pour s'enregistrer auprès du service d'authentification et qui stocke et exploite, typiquement au moyen d'un « cookie », les éléments nécessaires au dialogue entre le service d'authentification, l'utilisateur et les organismes qui demandent l'authentification. Cette application de la législation européenne couvre jusqu'à la communication de données par le service d'authentification à des organismes qui seraient établis dans des pays tiers.

On observera que selon la société Microsoft, le gouvernement américain estimerait que le service, parce qu'il est offert depuis les États Unis où les bases de données sont situées, serait régi par le droit américain. Lors d'une rencontre à Bruxelles en octobre 2002 avec le groupe dit « de l'article 29 », un représentant de la *Fédéral Trade Commission* (FTC) avait d'ailleurs indiqué qu'il serait beaucoup plus simple et efficace de considérer que seule la FTC, à l'exclusion donc des autorités européennes, serait compétente pour contrôler ce service. Il n'en demeure pas moins que la société Microsoft s'est déclarée prête à appliquer la législation européenne dès le mois de juillet 2002.

Les travaux du groupe dit « de l'article 29 », ainsi que les engagements pris par la suite par Microsoft d'apporter des modifications à son service selon un calendrier précis, ont été largement repris par la presse, tant en Europe qu'aux États Unis. On notera que l'attention du Parlement européen, et en conséquence celle de la Commission européenne, avait été attirée sur le service Net Passport par une question écrite d'un parlementaire néerlandais. De son côté la *Fédéral Trade Commission* américaine avait été saisie par de multiples associations de plaintes concernant, entre autres, les défauts de sécurité du service Passport. À cet égard, la FTC, à l'issue d'une longue enquête, avait publié en août 2002 un accord passé entre cette administration et Microsoft, en vertu duquel celle-ci s'engage pendant vingt-cinq ans à mettre en oeuvre toute une série de mesures destinées à assurer la sécurité du service (formation du personnel, plan sécurité etc.).

Il est intéressant de constater que les démarches entreprises en Europe sous l'empire de la directive 95/46/CE ont permis d'élargir les garanties offertes par ce service, particulièrement quant à la véritable transparence du fonctionnement du service vis-à-vis des internautes qui, ainsi, ne peuvent être soumis à des exploitations de leurs données sans en être informés au préalable, et sont également mis en mesure de décider quelles données peuvent être communiquées à des tiers, à quel moment et sous quelles garanties.

Chapitre 5

LISTES NOIRES : SUITE

Dans le rapport 2001 un long développement était consacré aux « listes noires » dans le secteur du crédit et celui de la téléphonie ainsi que dans des approches multisectorielles.

Pourquoi y revenir cette année et pour les mêmes secteurs, pour ne pas dire les mêmes sociétés ?

C'est essentiellement sous l'angle des plaintes que le présent chapitre reprend la question. Le nombre de ces plaintes qui se comptent en dizaines ou en centaines par an pourra paraître dérisoire au regard des milliers ou des centaines de milliers d'individus qui transitent dans ces traitements de lutte contre la fraude ou l'impayé. Pourra être tenu comme négligeable ou secondaire le fait que ces plaintes qui exigent une instruction minutieuse pour démêler la bonne de la mauvaise foi, l'incompétence de la volonté de punir mobilisent, à temps complet plusieurs agents publics au sein des services de la CNIL. Nul ne contestera cependant que les traitements mis en œuvre pour la gestion de ces listes noires sont, de manière exemplaire, révélateurs de la capacité de l'informatique en réseau à gérer des processus d'exclusion sociale. Cette préoccupation est largement partagée au sein de l'Union européenne, même si un débat est ouvert sur les risques comparés des deux techniques possibles de mutualisation de l'information financière personnelle : la centrale négative (tout ce que je dois) et la centrale positive (tout ce que je possède).

I. LE SECTEUR DE LA BANQUE, DU CREDIT ET DU RECOUVREMENT DE CRÉANCES

A. La CNIL en médiateur bancaire

La loi leur en faisant désormais obligation, les banques ont, dans la période récente, systématiquement mis en place des médiateurs chargés de traiter les litiges avec la clientèle. La CNIL ne peut que se réjouir de cette généralisation tant elle est appelée elle-même à intervenir dans ce rôle auprès des banques et des établissements de crédit.

1. L'EXERCICE DU DROIT D'ACCES

a) Le droit d'accès auprès des banques, des établissements de crédit et des services financiers de La Poste

Au cours de l'année 2002, la Commission a reçu de nombreuses plaintes de clients des banques, d'établissements de crédit et des services financiers de La Poste qui, ayant exercé leur droit d'accès auprès de ces organismes n'ont, soit pas obtenu de réponse, soit obtenu des réponses peu claires.

Dans les deux cas, la CNIL intervient.

Les articles 34 et suivants de la loi du 6 janvier 1978 reconnaissent à toute personne concernée par un fichier le droit d'obtenir une communication en langage clair des données la concernant qui y sont enregistrées.

Les données ainsi communiquées doivent être complètes et lisibles. Doivent, dès lors, être transmises au titulaire du droit d'accès toutes informations qui seraient enregistrées dans des « zones libres » (commentaires, par exemple), ainsi que la signification de tout code ou sigle associés à ces données.

M^me^ M. écrit à sa banque afin d'obtenir communication des informations la concernant enregistrées dans les fichiers de cet établissement, le segment de clientèle dans lequel elle serait classée, ainsi que tous commentaires qui pourraient être associés à la gestion de son compte.

Elle obtient de sa banque une copie des écrans informatiques comportant, certes, des informations la concernant, mais surtout de nombreux codes et sigles incompréhensibles : « origine : PAC DIST », « MAJ 10/200 », « CLT PR RA 05/09 : 1569,28 », « A C/05OU0696333 » etc.

M^me^ M. saisit la CNIL. La CNIL est intervenue auprès de sa banque afin que lui soit adressée la signification de l'ensemble de ces abréviations, sigles ou codes.

b) Le recours à des sociétés de garantie de paiement des chèques et l'exercice du droit d'accès

M. P. vient de faire ses courses dans une grande surface et s'apprête à payer par chèque le montant de ses achats. M. P. est stupéfait, son chèque n'est pas accepté. « La machine » le refuse alors que son compte bancaire n'est pas à découvert.

La mésaventure de M. P. est loin d'être un cas isolé. La réponse de la « machine » provient de la consultation par la grande surface d'une application informatique mise à sa disposition par une société de garantie de paiement des chèques.

Les particuliers sont souvent mal informés sur la possibilité reconnue à toute personne à laquelle est remis un chèque pour le paiement d'un bien ou d'un service, directement ou par l'intermédiaire d'un mandataire, de vérifier auprès de la Banque de France si ce chèque n'a pas été déclaré comme volé ou perdu, n'a pas été tiré sur un compte clôturé ou émis par une personne frappée d'une interdiction judiciaire ou bancaire.

Beaucoup de commerçants ne procèdent pas eux-mêmes à cette vérification mais font appel à des sociétés de garantie de chèques qui effectuent, par ailleurs, une évaluation statistique du fonctionnement du chéquier et attribuent une sorte de *« scoring »* du paiement par chèque (réalisation de statistiques sur la fréquence d'utilisation d'un chéquier, à partir de chèques émis au cours d'une période donnée).

Ainsi, la société de garantie de chèques, à laquelle adhère la grande surface où M. P. faisait ses courses, a estimé que le nombre de chèques qu'il avait émis au cours d'une période donnée a pu faire craindre un risque potentiel d'utilisation frauduleuse de son chéquier. La grande surface a donc préféré ne pas prendre ce risque et refuser le chèque de M. P. Si elle l'avait accepté, le paiement du chèque n'aurait pas été garanti par la société dont elle est adhérente.

Les clients disposent d'un droit d'accès qui s'exerce auprès de ces sociétés de garantie de paiement des chèques et doivent être informés lors du passage en caisse que le magasin recourt à un tel système.

La CNIL rappelle ces éléments aux personnes qui la saisissent et les informe qu'en tout état de cause un commerçant est libre de refuser un paiement par chèque.

2. LES REFUS DE CREDIT

Comme les années précédentes, beaucoup de personnes se sont tournées vers la CNIL en 2002 pour contester leur inscription au fichier national des incidents de remboursement des crédits aux particuliers (FICP) effectuée par leur banque ou un organisme de crédit. La CNIL a également été souvent interrogée par des personnes qui, s'étant vu refuser un crédit, s'interrogent sur les motifs de ce refus et leur possible « fichage » dans des « listes noires ».

Le fichier national des incidents de remboursement des crédits aux particuliers (FICP) est géré par la banque de France et recense l'ensemble des impayés de crédit dans le but de prévenir les cas de surendettement. La CNIL est fréquemment

saisie par des personnes qui contestent leur inscription, effectuée par une banque, un organisme de crédit ou les services financiers de La Poste, au FICP.

Pour l'année 2002, la CNIL a obtenu, dans une quarantaine de cas, la radiation d'une personne du FICP, parce que son fichage n'était pas ou plus, justifié.

Tel a été le cas pour M. F., inscrit au FICP par son établissement bancaire plus de sept ans après que l'incident de paiement a été constaté par la banque.

Tel a été le cas également de M^me^ D., qui a eu des retards dans le remboursement de son crédit contracté auprès d'une banque mais a régularisé très rapidement l'incident (dans le délai d'un mois). Or, la banque a maintenu son fichage au FICP pendant dix-huit mois après la régularisation de l'incident, et n'a « défiché » M^me^ D. qu'après l'intervention de la CNIL.

Tel a encore été le cas de M^me^ M. qui, alors qu'elle avait remboursé son crédit par anticipation en janvier 2002, a été inscrite au FICP par l'établissement de crédit en juin 2002, à la suite d'un « dysfonctionnement » dans le traitement de son chèque de remboursement. Malgré les courriers de réclamation qu'elle a adressés à cet établissement, elle n'a été « défichée » qu'après l'intervention de la CNIL.

Face à l'incompréhension des particuliers à l'égard des mécanismes qui conduisent à un refus de crédit, la CNIL a élaboré un guide pratique à leur intention.

Ce guide[1] fournit des renseignements pratiques aux personnes sur les règles de fonctionnement du FICP, les méthodes des banques et établissements de crédit (telles que le score ou les règles de fichage interne) et les droits que peuvent exercer les personnes sur le fondement des dispositions de la loi du 6 janvier 1978 : droit d'accès, de rectification, possibilité de saisir la CNIL.

L'action quotidienne de la CNIL au service des victimes d'un système qui, il faut le rappeler si besoin était, a sa justification pour limiter le surendettement et prémunir les établissements de crédit contre les mauvais payeurs serait de faible portée si la Commission n'avait pas le souci de limiter et d'encadrer les outils de sélection voire d'exclusion qu'une partie du secteur bancaire et financier souhaiterait mettre en place.

B. La mutualisation des informations financières sur les particuliers

Le rapport 2001 avait déjà largement abordé la question des « listes noires » à l'occasion de l'apparition d'acteurs forts sur un marché en pleine expansion. Il n'y a pas grand risque à parier que le rapport 2003 reviendra sur le sujet avec les conclusions du groupe de travail constitué sur ce sujet au sein de la CNIL. L'année 2002 apparaît dès lors comme une année de transition : les traitements s'installent et les débats se poursuivent sur les avantages et les inconvénients des centrales négatives ou positives.

[1] Accessible sur le site internet de la CNIL : www.cnil.fr

1. UN « SERVICE DE PREVENTION DU SURENDETTEMENT »

La CNIL a examiné lors de sa séance plénière du 19 novembre 2002 une déclaration ordinaire d'un traitement automatisé d'informations nominatives relatif à un « service d'information pour la prévention du surendettement » mis en œuvre par la société commerciale Experian, société spécialisée dans le traitement de l'information et qui développe des centrales d'information sur les particuliers dans plusieurs pays européens.

Il ressort de la déclaration que le traitement fournit aux adhérents de la centrale des indicateurs caractérisant le niveau d'endettement d'une personne à partir de la centralisation des prêts consentis à la personne concernée, ainsi que le nombre et la nature des crédits souscrits.

Ce traitement s'inscrit ainsi dans le développement d'une « centrale d'informations » offrant aux professionnels du crédit adhérents l'accès à des outils d'analyse et de comparaison portant sur les informations communiquées par une personne lors de la présentation d'une demande de crédit. Le traitement des « incohérences » et la mutualisation de ce traitement au profit de l'ensemble des adhérents de la « Centrale » d'Experian ont fait l'objet d'un examen par la Commission en 2001 (cf. rapport d'activité 2001 pp. 147-152).

La Commission a estimé que l'ouverture d'un « service » destiné à fournir des informations sur le niveau d'endettement des clients constituait ce qu'il est convenu d'appeler un « fichier positif », qui, par opposition aux « fichiers négatifs » qui ne comportent que des informations sur des défauts de paiement, rassemble des informations sur les encours de crédit ou la situation du débiteur en général. Or, à plusieurs reprises, la CNIL a exprimé son opposition à la constitution de fichiers positifs regroupant les encours de crédit en raison du risque d'atteinte à la vie privée présenté par ces fichiers qui contiennent plus de données que les fichiers négatifs relatifs aux incidents de paiement et se prêtent plus facilement qu'un fichier négatif à des détournements de finalité et notamment à un ciblage commercial.

En outre, dans la mesure où le secteur du crédit est régi par le secret bancaire, la centralisation et l'accessibilité par des tiers à des informations nominatives couvertes par le secret professionnel soulèvent une autre difficulté. Le dossier de déclaration examiné par la CNIL précise à cet égard qu'il revient à chaque adhérent d'obtenir préalablement à l'enregistrement de tout dossier dans la base centrale la levée du secret bancaire par la personne concernée.

Il apparaît toutefois que seule une intervention législative est de nature à permettre une dérogation aussi large au principe du secret bancaire tel que posé par les dispositions des articles L. 511-33 et L. 511-34 du Code monétaire et financier, notamment pour des conventions ayant le caractère de contrats d'adhésion où par définition le pouvoir de négociation du particulier est extrêmement faible, où le droit d'opposition ne peut être réellement exercé et où la souscription d'une clause particulière ne permet pas d'assurer que la personne a indubitablement donné son consentement, de façon libre et éclairée.

Enfin, le recensement dans une même base de données de l'ensemble des informations relatives à l'endettement pose la question de la définition des éléments qui devront être pris en compte pour arrêter le niveau d'endettement de la personne, la multiplication des cartes de paiement associées à un crédit renouvelable ne donnant pas l'état réel de l'endettement d'une personne.

Il est apparu à la Commission qu'un fichier centralisant des informations relatives aux crédits demandés ou souscrits par les particuliers, s'il s'avérait indispensable à la profession et socialement admis, ce qui ne lui semble pas être le cas, devrait faire l'objet d'un encadrement législatif précis du fait des risques d'atteinte à la vie privée, des contraintes liées à l'application du secret bancaire et de la nécessaire proportionnalité des traitements au regard de la finalité poursuivie. Devraient ainsi être définies les conditions d'inscription dans un tel fichier, la durée de conservation des données et les modalités pratiques d'exercice de leurs droits par les personnes concernées. Au surplus, un tel fichier devrait être régi par des contraintes de service public, même s'il était exploité par une société privée.

La procédure applicable aux fichiers privés étant celle d'une simple déclaration à la CNIL contre délivrance d'un récépissé, la Commission ne dispose pas, sur le fondement de la loi du 6 janvier 1978, du droit de s'opposer à la mise en œuvre de tels fichiers ni de celui de subordonner leur existence à certaines conditions de fonctionnement. Elle a donc délivré un récépissé à la société concernée. La Commission a toutefois estimé nécessaire d'alerter les pouvoirs publics, en l'espèce le Premier ministre, les commissions des lois de l'Assemblée nationale et du Sénat et enfin le Comité de réglementation bancaire.

2. LE CONTRÔLE EFFECTUÉ AUPRÈS DE LA SOCIÉTÉ EXPERIAN

Par délibération n° 02-023 du 2 avril 2002, la CNIL a décidé d'effectuer un contrôle auprès de la même société Experian afin de s'assurer du respect par cette société des dispositions de la loi du 6 janvier 1978 dans le cadre de la mise en œuvre d'un traitement relatif à la mutualisation des incohérences dans les demandes de crédit. Le contrôle a eu lieu le 11 juillet 2002 auprès de l'établissement où se situent les installations informatiques de la société et les équipes responsables des traitements.

La société Experian centralise les demandes de crédit adressées par les établissements de crédit adhérents. La base ainsi constituée permet d'effectuer des contrôles de « cohérence » sur les nouvelles demandes par comparaison avec celles présentées précédemment par un même demandeur soit auprès d'un même établissement de crédit, soit auprès de plusieurs adhérents de la Centrale ayant décidé de mettre en commun les demandes de crédit traitées. Au jour du contrôle 1 394 000 demandes de crédit étaient recensées dans la base.

Afin d'assurer le respect de la finalité du traitement, les établissements de crédit adhérents n'ont pas accès à la base mutualisée, mais uniquement aux alertes générées à leur requête sur des demandes de crédit qu'ils sélectionnent. En outre, l'exhaustivité des renseignements demandés permettrait de s'assurer qu'une

demande de crédit est bien à la source de l'interrogation. Il est apparu toutefois à la Commission que cette pratique n'est pas conforme aux dispositions de l'article 5 de la convention 108 du 28 janvier 1981 du Conseil de l'Europe aux termes duquel seules les données « pertinentes, adéquates et non excessives » par rapport à la finalité déclarée peuvent faire l'objet d'un traitement. La Commission a ainsi estimé que le manque de pertinence de la conservation des données ne faisant pas l'objet d'un contrôle de cohérence doit conduire à la mise en place de procédures d'effacement de ces données lors de la transmission ou après apurement de la base et qu'une journalisation des requêtes et règles produites par le traitement était de nature à rendre effective la prise en compte du risque de détournement de finalité par les adhérents.

Pour permettre un contrôle par les titulaires du droit d'accès de l'utilisation faite des données les concernant, la Commission a estimé qu'il pourrait être envisagé de faire figurer dans le relevé d'informations fourni en réponse à une demande d'accès les coordonnées des organismes ayant successivement enrichi !a base et reçu des informations en retour sous forme de codes de détection d'incohérence. Dans le cas du fichier national des chèques irréguliers géré par la Banque de France, une telle procédure permet une information totale de l'intéressé puisque ces informations figurent dans le relevé transmis aux personnes concernées à l'occasion de l'exercice de leur droit d'accès.

S'agissant de l'information des personnes, la Commission a estimé, dans la mesure où le préalable indispensable à une mutualisation d'informations couvertes par le secret bancaire est l'acceptation indubitable et éclairée par le demandeur de crédit du partage d'informations, une clause conventionnelle devra imposer aux adhérents la désignation de la société Experian en tant que destinataire des informations dans la clause d'information préalable contenue dans la zone d'acceptation de la demande de crédit.

Enfin, la mutualisation exposée dans la déclaration de la société Experian n'étant pas effective au jour du contrôle, la Commission suivra avec attention les déclarations adressées par les adhérents de la Centrale de la société Experian et décidera s'il y a lieu de nouvelles mesures d'investigation tant auprès des adhérents que d'Experian afin de s'assurer de la mise en oeuvre effective des garanties présentées.

3. L'AUTOPROCLAME « FICHIER NATIONAL DES INCIDENTS DE PAIEMENT »

Par délibération n° 01-063 du 13 novembre 2001, la Commission a décidé de procéder à une mission de contrôle auprès de la société BGD qui a déclaré un traitement relatif à une banque télématique d'informations sur des débiteurs dénommée fichier national des incidents de paiement (FNIP), une appellation particulièrement contestable puisque laissant à penser à tort que cet organisme est officiel. Ce contrôle, qui s'est déroulé le 29 janvier 2002 prend place dans le cadre d'une étude d'ensemble de la Commission sur la question des fichiers ayant pour objet le rensei-

gnement commercial, le recouvrement de créance ou la mutualisation de renseignements relatifs au comportement de clients.

La société BGD avait retenu lors de la présentation du traitement en 2000 la sectorisation du fichier pour les créances civiles avec trois secteurs : l'immobilier, la téléphonie et l'assurance. Les opérations de contrôle ont permis de vérifier l'effectivité de la sectorisation par branche d'activité.

S'agissant de l'information des personnes, la Commission a pu vérifier que la formulation qu'elle avait préconisée a été retenue par la société BGD. Toutefois, les adhérents ne sont pas invités à rappeler aux personnes fichées le droit d'accès et de rectification. Le rappel de ces droits ainsi que de la faculté de s'opposer pour motif légitime ne figure que sur le premier courrier adressé par la société BGD.

La procédure d'inscription d'une personne dans le fichier comprend :
— une mise en demeure du créancier ou de son mandataire mentionnant le fait que la société est adhérente au FNIP et qu'elle a, à ce titre, obligation de déclarer tous ses impayés sur ce fichier dans un délai de quinze jours ;
— un préavis d'inscription lequel mentionne qu'à défaut de règlement ou de contes tation motivée et justifiée, il sera procédé à l'inscription dans le fichier à l'issue d'un délai de huit jours ;
— enfin la dernière étape épistolaire est constituée par l'avis d'inscription.

La société BGD a également inclus dans ses conditions générales de vente la nécessité de ne procéder qu'à l'inscription de créances certaines, liquides et exigibles.

D'une façon générale, la société BGD a ainsi respecté les éléments de sa déclaration et tenu compte des préconisations de la Commission, hormis en ce qui concerne la référence qu'elle fait abusivement à un prétendu agrément de la CNIL. La Commission a demandé sur ce point à cette société de modifier les pages litigieuses de son site internet.

Toutefois, les opérations de contrôle ont mis en évidence que l'architecture informatique retenue par la société BGD présente l'inconvénient de conserver les informations sur l'identité des personnes physiques ayant été débitrices à un moment donné. Bien que cette inscription ne soit plus consultable par les adhérents, l'identité des débiteurs reste connue de la société BGD et la base centralise ainsi toutes les personnes ayant été débitrices à un moment donné. La Commission a estimé que le simple fait de figurer dans la base constitue un fichage en tant que mauvais payeur et ce d'autant que la base de données recensant les personnes enregistrées est ouverte aux cabinets de recouvrement de créances qui l'utilisent comme un annuaire ouvert aux cabinets souhaitant vérifier les coordonnées d'un débiteur. La commission a donc demandé à la société BGD d'apurer la base des informations relatives à l'identité des débiteurs après la radiation de l'inscription, une telle conservation n'étant pas conforme à la déclaration de traitement auprès de la CNIL, ni aux dispositions de la loi du 6 janvier 1978.

II. LE FICHIER PREVENTEL : LA CNIL EN SERVICE APRÈS-VENTE DE LA TÉLÉPHONIE MOBILE

Comme elle l'avait annoncé lors de son rapport annuel précédent, la Commission a exercé, au *cours* de l'année 2002, un contrôle très attentif aux conditions de mise en œuvre du fichier recensant les impayés dans le secteur de la téléphonie.

Il faut rappeler que les opérateurs de téléphonie mobile (SFR, Orange et Bouygues Télécom) et certains opérateurs de téléphonie fixe se sont regroupés au sein d'un groupement d'intérêt économique (GIE) dans le but de mettre en œuvre un traitement (« Preventel ») de prévention des impayés dans le secteur des télécommunications par la centralisation d'informations relatives à des impayés et des anomalies constatés auprès de leurs abonnés, survenant lors de la souscription ou de l'exécution des contrats d'abonnement tant particuliers qu'entreprises.

Il n'est pas inutile d'expliquer avec précision le fonctionnement de ce fichier.

A. Caractéristiques du fichier Preventel

Qu'est ce que le fichier Preventel ?	C'est un fichier qui recense les impayés dans le secteur de la téléphonie mobile et fixe. Il est mis en œuvre par le GIE Prévention Télécommunications (Gie preventel).
A quoi sert le fichier Preventel ?	Les membres du GIE Preventel interrogent le fichier chaque fois qu'une personne souhaite souscrire un abonnement téléphonique. Si la personne est fichée, l'abonnement lui est refusé ou un dépôt de garantie lui est demandé.
Quels sont les membres du GIE Prevenfel ?	— Les opérateurs de téléphonie mobile : Bouygues Telecom, Orange France, SFR. — Les sociétés qui commercialisent les services de ces opérateurs : Carrefour Telecom, Cmc, Coriolis Telecom, Debitel France. — Certains opérateurs de téléphonie fixe.
Qui peut être inscrit dans le fichier Preventel ?	— Les abonnés à un téléphone mobile ou fixe débiteurs d'une somme supérieure ou égale à 60 €. — Les personnes qui auraient souscrit irrégulièrement un contrat d'abonnement auprès d'un ou plusieurs opérateurs en produisant, par exemple, des documents d'identité ou bancaires falsifiés.
Qui peut inscrire les abonnés dans le fichier Preventel ?	Les membres du GIE Preventel.

Quelles sont les informations inscrites dans le fichier Preventel ?	— Pour les personnes physiques : le nom, le prénom, le sexe, la date et le lieu de naissance. — Pour les personnes morales : le numéro Siren, le nom ou raison sociale et l'adresse. — Dans fous les cas : le codage de l'anomalie (« impayé » ou « anomalie sur les documents présentés » ou « usurpation d'identité), le membre du GIE Preventel ayant procédé à l'inscription et la date de cette inscription.
Qui peut accéder aux informations enregistrées dans le fichier Preventel ?	Le GIE Preventel et les services des membres du GIE Preventel chargés de la gestion des abonnements et des recouvrements.
Quand les informations sont-elles supprimées du fichier Preventel ?	Dès le règlement complet de la dette (le membre du GIE Preventel à l'origine de l'inscription effectue la main levée). — En tout état de cause, à l'expiration d'un délai de 3 ans (ce délai est porté à 5 ans lorsque la personne physique ou morale concernée rail l'objet d'au moins trois inscriptions, simultanément, à une date donnée).
Où une personne physique doit-elle s'adresser pour exercer son droit d'accès aux données la concernant qui seraient enregistrées dans le fichier Preventel ?	Par courrier au GIE Preventel, service des consultations - Tsa n° 90 003, 93588 Saint-Ouen Cedex (joindre une copie d'une pièce d'identité ou préciser son identité, ses date et lieu de naissance).
Recommandations de la CNIL	— Les personnes doivent être informées de l'existence et du fonctionnement du fichier Preventel par une mention portée sur les formulaires de prise d'abonnement, ainsi que sur le contrat qu'elles souscrivent. — Aucune inscription ne peut être effectuée sans que les personnes concernées aient été préalablement informées et mises en mesure de régulariser leur situation. — En cas de contestation par leurs clients des créances réclamées, les membres du GIE Preventel doivent établir le bien fondé de leur demande de paiement, par une instruction contradictoire de la contestation, conduite dans un délai raisonnable, de façon non automatisée, assortie de la suspension du processus d'inscription dans le fichier.
Numéro de récépissé de déclaration à la CNIL	n° 488814 délivré le 20 janvier 1997 - récépissé de modification délivré le 29 avril 2002.

B. Les plaintes

Compte tenu du nombre élevé de plaintes émanant de particuliers relatives à l'existence ou à la tenue du fichier Preventel, la Commission avait décidé, en 2000, une mission de contrôle qui a conclu au nécessaire rappel des conditions dans lesquelles un tel fichier devait être géré.

Suite à la déclaration modificative apportée à ce fichier l'année dernière (abaissement du seuil de l'impayé pouvant justifier une inscription, extension de ce fichier aux opérateurs de téléphonie fixe, allongement de la durée d'inscription en cas d'inscription multiple), la Commission a souhaité établir un bilan des plaintes dont elle a été saisie et entendre l'ensemble des membres du GIE Preventel afin que soient apportées, dans les meilleurs délais, les modifications nécessaires à une meilleure mise en œuvre de ce fichier.

Le bilan du nombre de plaintes reçues par la Commission concernant la gestion du fichier Preventel est en augmentation. Ainsi, 43 réclamations ont été traitées au cours de l'année 2000, 88 au cours de l'année 2001 et 1 32 au cours de l'année 2002. S'ajoutent à ces saisines, de nombreux appels téléphoniques quotidiens.

Si quelques-uns des 132 courriers (une vingtaine) concernant le fichier Preventel, reçus par la CNIL en 2002, ne sont que de simples demandes d'informations de particuliers sur les caractéristiques du fichier Preventel, les autres révèlent dans leur grande majorité des dysfonctionnements concernant l'alimentation et la consultation du fichier par les opérateurs de téléphonie mobile.

1. LES PLAINTES RELATIVES A L'ALIMENTATION DU FICHIER PREVENTEL

La majorité des plaintes reçues par la CNIL émanent d'abonnés à un opérateur de téléphonie qui contestent soit le bien-fondé, soit le montant de la somme qui leur est réclamée et qui a donné lieu à leur inscription dans le fichier Preventel.

Déjà saisie de ce type de plaintes en 2000 et en 2001, la CNIL avait demandé au GIE Preventel que la situation des clients contestants le montant ou le fondement juridique de la somme dont le paiement leur était réclamé, fasse l'objet d'un examen attentif par les opérateurs qui sollicitent leur inscription dans le fichier.

La Commission considère que ces contestations doivent faire l'objet d'une instruction contradictoire, conduite dans un délai raisonnable, de façon non automatisée, assortie de la suspension du processus d'inscription dans le fichier Preventel.

Il convient de rappeler que les tribunaux judiciaires sont seuls compétents pour trancher une contestation sur le caractère certain, liquide et exigible d'une créance.

Par ailleurs, et dans de nombreux cas, les plaintes d'abonnés contestant la dette à l'origine de leur inscription dans le fichier Preventel témoignent de ce qu'ils ont tenté à plusieurs reprises de faire valoir leurs observations auprès de leur opérateur (par courriers simples, lettres recommandées, appels téléphoniques) sans jamais obtenir de réponse. C'est en dernier recours qu'ils s'adressent à la Commission.

Par exemple, M. G. a résilié, au mois de janvier 2002, son contrat d'abonnement de téléphonie mobile souscrit en 2000. En février 2002, son opérateur l'informe qu'il est redevable d'une somme de 120 euros au titre d'un préavis de deux mois restant à courir.

Or, M. G. conteste ce préavis et, en conséquence, la créance que lui réclame son opérateur au titre de ce préavis. Il lui écrit pour protester et fait opposition aux prélèvements bancaires de son abonnement.

M. G. reçoit plusieurs relances de paiement puis est informé, au mois de juin 2002, de son inscription dans le fichier Preventel. En revanche, et malgré un nouveau courrier à son opérateur, M. G. ne reçoit aucune réponse s'agissant des éléments de sa contestation.

M. G. écrit donc à la Commission qui intervient auprès de l'opérateur. Ce dernier reconnaît enfin que ses nouvelles conditions d'abonnement ne s'appliquaient pas au contrat de M. G., annule la dette et supprime son inscription du fichier Preventel.

Le cas de M^{me} B. est tout aussi illustratif.

En janvier 2002, elle conteste auprès de son opérateur le montant de certaines factures et fait opposition aux prélèvements bancaires de son abonnement. Pour toute réponse, elle est informée de son inscription dans le fichier Preventel.

M^{me} B. écrit à son opérateur, sans succès, puis saisit la CNIL.

L'opérateur répond enfin. Il reconnaît le bien-fondé de la contestation de M^{me} B., procède à la régularisation de la facturation et supprime son inscription du fichier Preventel.

2. LES PLAINTES RELATIVES A LA CONSULTATION DU FICHIER PREVENTEL

L'instruction d'autres plaintes ont révélé que, lors d'une demande de souscription de contrat, les services des opérateurs consultant le fichier Preventel avaient estimé que l'information, fournie par le GIE Preventel, selon laquelle les données communiquées pour la consultation du fichier permettaient d'indiquer qu'il existait des réponses « phonétiquemenf approchée » ou une réponse se rapportant à un « *homonyme né le même jour mais dans un autre département »,* empêchait la souscription du contrat ou subordonnait l'abonnement à la remise d'un dépôt de garantie.

C'est ainsi que M. L. qui souhaite souscrire pour la première fois un contrat d'abonnement de téléphonie mobile se rend dans un point de vente.

Le personnel de ce point de vente lui indique que l'opérateur refuse de lui ouvrir une ligne au motif que ses coordonnées figurent dans le fichier Preventel. M. L., surpris, écrit au GIE Preventel qui lui répond que ses coordonnées ne figurent pas dans le fichier Preventel.

Il saisit la Commission qui interroge l'opérateur concerné. Cet opérateur confirme que M. L. n'est pas inscrit dans le fichier Preventel et l'invite à renouveler sa demande d'abonnement.

M. L. a très vraisemblablement été « victime » d'une mauvaise lecture, par les services de l'opérateur concerné, communiquée au point de vente, des informations enregistrées dans le fichier Preventel.

M ^{e} M. souhaite également souscrire pour la première fois un contrat de téléphonie mobile. Un refus lui est opposé au motif qu'elle est inscrite dans le fichier Preventel. M M. écrit au GIE Preventel qui lui indique qu'il existe une *« M^{lle} M. née le même jour mais dans un autre département »* fichée dans Preventel.

Les plaintes reçues par la Commission témoignent dans leur grande majorité des difficultés auxquelles se heurtent les abonnés pour trouver des interlocuteurs au sein des différents services des opérateurs.

La Commission ne peut qu'observer que ces difficultés sont le résultat de dysfonctionnements des services juridiques, commerciaux ou de recouvrement des opérateurs de téléphonie (absence de gestion et de coordination entre ces services).

L'accroissement des utilisateurs de téléphonie mobile devrait conduire les membres du GIE Preventel à renforcer les procédures d'examen des situations des abonnés qui s'adressent à leurs services pour contester les créances qui leur sont réclamées. Un tel renforcement se révèle indispensable pour que le processus d'inscription des personnes dans le fichier Preventel, qui demeure un fichier d'exclusion, cesse d'être automatisé.

3. LES ENGAGEMENTS DE PREVENTEL

Face au constat fait par la CNIL, les membres du GIE se sont engagés sur un certain nombre de points.

En premier lieu, les opérateurs se sont engagés sur une amélioration du traitement des litiges liés au fichier Preventel. À cet effet, des correspondants CNIL seront mis en place au sein de chacun des opérateurs et auront la charge de traiter les éventuelles contestations. Une procédure d'information du GIE Preventel par la Commission sera mise en place afin que le GIE puisse établir une typologie des saisines traitées par la CNIL et des réponses qui y sont apportées. Le GIE s'est engagé à rendre compte à ses membres des dysfonctionnements dont il aura ainsi connaissance afin de leur permettre, le cas échéant, de prendre les mesures appropriées.

En second lieu, le fonctionnement global du fichier Preventel doit être amélioré. La fonction dite du « phonétiquement approché » doit être refondue pour affiner les réponses et, surtout, n'être que l'indicateur d'une possible falsification d'identité et, en aucun cas, conclure à une inscription de la personne concernée. Les conditions d'inscription, tant au niveau du seuil que de la durée, seront, quant à elles, rappelées. Les contestations relatives au caractère certain, liquide et exigible de la créance devront donner lieu à une suspension de l'inscription et à étude personnalisée du dossier.

Ces mesures sur lesquelles le GIE et les opérateurs se sont aussi engagés doivent être rappelées dans des consignes qui seront adressées, depuis le plus haut niveau, aux services de chacun des opérateurs et aux points de vente qui alimentent et consultent le fichier Preventel.

L'efficacité de ces mesures devra être démontrée par une baisse significative du nombre de réclamations dont est saisie la Commission. À défaut, la Commission serait alors fondée à rappeler au GIE, selon la forme qu'elle aura choisie, les obligations qu'impose la gestion d'un fichier dont la sensibilité particulière ne fait pas de doute.

III. LES LISTES NOIRES ET L'EUROPE

Les « listes noires » et particulièrement les fichiers de mauvais payeurs font partie de ces phénomènes qui ont participé, à l'origine, à faire se développer les règles de protection des données à caractère personnel dans le monde. À titre d'exemple, l'on peut rappeler que la première loi au monde ayant posé le principe du droit d'accès des personnes à leurs données est la loi dite *« Fair Crédit Reporting Act »* (FCRA), adoptée en 1970 aux États Unis, qui encadre les activités de gestion de listes de personnes à l'usage, entre autres, d'organismes de crédit.

Compte tenu des problèmes que pose la mise en œuvre de telles listes en Europe, il était naturel que le groupe de l'article 29 aborde ces questions, ce qu'il a fait courant 2002 dans un document de travail qui sera présenté en premier lieu. L'importance d'une vision européenne sur ces questions s'avère d'autant plus cruciale que l'on assiste au développement d'opérateurs internationaux, comme par exemple Experian, dont les activités ne se limitent plus au territoire d'un seul État.

Ces travaux du groupe prennent une résonance particulière dans le contexte actuel des travaux de la Commission européenne, qui a présenté dans le courant de 2002 une proposition de directive dans le domaine du crédit à la consommation. En effet, une des implications de cette proposition de directive concerne précisément l'institution au moins d'une liste noire de mauvais payeurs dans ce domaine. Le groupe de l'article 29 a bien évidemment été saisi de ces travaux. À cette occasion, le groupe a rendu un avis sur la proposition de la Commission.

A. Front commun sur les listes noires

Après avoir comparé de manière détaillée les différentes expériences des autorités européennes de protection des données en la matière, le groupe de l'article 29 a adopté, lors de sa séance du 3 octobre 2002, un document de travail sur les fichiers dits de « listes noires ».

En effet, si ces fichiers de « personnes indésirables » ont une utilité sociale et économique incontestable, en revanche, leur existence, et plus particulièrement celle de fichiers mutualisés d'impayés ou de prévention de la fraude comporte des risques sérieux d'exclusion et de marginalisation des personnes concernées : une personne fichée peut alors se voir refuser un crédit, un logement, un emploi, etc., du fait de son inscription sur une liste. Il s'est avéré, à l'occasion de ces travaux du groupe, que tous les pays d'Europe étaient concernés par cette problématique.

Dans ce contexte, il est apparu essentiel au groupe de faire un état des lieux des questions posées par cette problématique en Europe, ainsi que d'adopter des principes et des critères communs à la tenue de tels fichiers. L'objectif de cette démarche, conformément aux missions du groupe, était de permettre que les personnes fichées dans de telles listes noires puissent se voir reconnaître les mêmes droits et garanties dans tous les pays de l'Union au regard de la protection de leurs données personnelles.

Au préalable, le document du groupe rappelle que le concept de liste noire recouvre des réalités extrêmement diverses. Le document offre une définition de ce concept : une liste noire consiste ainsi « à *collecter et à diffuser certaines informations concernant un groupe donné de personnes, élaborées conformément à certains critères en fonction du type de liste noire dont il s'agit, se traduisant en règle générale par des effets nocifs et préjudiciables pour les personnes qui y figurent ».* Plus particulièrement, *« ces effets peuvent entraîner la discrimination d'un groupe de personnes en les privant de toute possibilité d'accès à un service déterminé ou en nuisant à leur réputation ».*

Les fichiers de mauvais payeurs ou de fraudeurs ne sont donc qu'une des multiples applications de ces listes, et la définition donnée englobe également de nombreux cas de figure (fichiers d'infractions administratives, listes relatives aux négligences professionnelles ou listes incluant des données sur certains comportements individuels considérés comme inadéquats par certains secteurs sociaux, etc.). Chacun de ces cas fait l'objet de recommandations propres dans le document du groupe.

En pratique, il apparaît que le plus grand nombre de problèmes posés par ces listes noires concerne les fichiers de mauvais payeurs ainsi que les fichiers d'appréciation de la solvabilité patrimoniale des personnes dans le domaine du crédit (cette seconde formulation se rapportant aux activités d'origine américaine dites de *« crédit referencing »).* Cette dernière pratique n'existant pas en France, l'utilité essentielle du document du groupe sur ces questions concerne donc les fichiers dits « d'impayés ».

Il convient de rappeler, comme il a été dit précédemment dans ce chapitre, que les fichiers d'impayés suscitent un grand nombre de plaintes auprès de la CNIL, et que ce phénomène est commun à tous les homologues européens de la Commission. Ce phénomène risque de s'amplifier avec le fait que, de plus en plus fréquemment, ces fichiers d'impayés sont mutualisés entre différents opérateurs et que cette mutualisation pourra concerner, à terme, des acteurs étrangers. L'opportunité de la démarche du groupe de l'article 29 consistant à poser des principes et des critères communs de fonctionnement à de tels fichiers apparaît ainsi de manière évidente.

En pratique, les recommandations émises par le groupe se recoupent parfaitement avec les principes et critères énoncés de longue date par la CNIL en matière de fichiers mutualisés d'impayés, notamment sur l'information des personnes (ce que la CNIL exprime très concrètement par la formule : *« les listes noires ne peuvent être secrètes »),* sur l'exigence de pertinence des informations enregistrées dans le fichier

et les conditions dans les lesquelles des informations doivent être enregistrées dans le fichier.

Au titre des préconisations relatives à ces conditions d'inscription, le groupe relève entre autres les éléments suivants : des créances impayées ne peuvent *être* inscrites que si la dette est certaine, c'est-à-dire que les conditions de son paiement par le débiteur sont supposées remplies ; il est également impératif que les informations figurant dans le fichier soient exactes et mises à jour, ce qui implique notamment que les inscriptions dans la base soient soumises à des durées de conservation prédéfinies ; les responsables de ces listes doivent assurer la sécurité et la confidentialité des données, ce qui implique en particulier que soient déterminées très précisément les conditions d'accès à ces fichiers, et ce tout particulièrement dans le cas de listes noires mutualisées.

Compte tenu de l'importance des enjeux que représentent ces fichiers pour les droits et libertés des personnes, le groupe conclut ce document par le souhait que les institutions communautaires prennent conscience de la nécessité de suivre l'orientation définie par ces développements. Ce souhait s'avère d'autant plus opportun qu'il intervient au moment de la publication d'une proposition de directive en matière de crédit à la consommation, qui prévoit, entre autres, la mise en place de bases centralisées de données relatives aux retards et incidents de paiement des particuliers.

B. La proposition de directive sur les crédits à la consommation

Le groupe de l'article 29 a rendu le 2 juillet 2002 un avis[1] sur une proposition de directive de la Commission dans le domaine du crédit à la consommation[2].

Cette directive volumineuse, dont le champ d'application est spécifiquement restreint au secteur du crédit à la consommation, a pour objectif général de permettre aux consommateurs et aux entreprises de tirer pleinement bénéfice du marché intérieur en matière de crédit. À cet effet, elle vise à harmoniser les conditions de protection des consommateurs dans le domaine, ainsi qu'à créer les conditions pour un marché du crédit à la consommation plus transparent et plus efficace.

A ce dernier titre, une des lignes directrices des rédacteurs de la proposition est de « *mettre en place un cadre structuré d'information du dispensateur de crédit, afin de lui permettre de mieux apprécier ses risques* »[3]. Un des moyens retenus par la proposition de directive pour assurer cette information consiste à instituer une base de données centralisées de type négatif, reprenant les retards et incidents de paiement, permettant d'identifier les consommateurs et les garants, couvrant au moins le

[1] Avis 3/2002 sur les dispositions en matière de protection des données d'une proposition de directive de la Commission sur l'harmonisation des lois, réglementations et dispositions administratives des ‹tats mem bres concernant les crédits à la consommation.

[2] Proposition de directive de la Commission sur l'harmonisation des lois, réglementations et dispositions administratives des Etats membres concernant les crédits à la consommation, 11 septembre 2002, COM [2002) 443 final.

[3] Exposé des motifs, p. 5.

territoire de l'État membre et assurant un accès à tous les prêteurs. L'article 8 rend cette base de données obligatoire et introduit un socle commun d'accès, de traitement et de consultation des données.

L'avis du groupe de l'article 29 a été rendu suite à sa consultation par la Commission sur cette proposition de directive, en vertu des procédures habituelles en la matière. Dans cet avis, le groupe a demandé que soit fait référence dans le texte aux dispositions de la directive 95/46/CE ou bien que des dispositions plus élaborées relatives à la protection des données y soient incorporées. La Commission aurait retenu une solution intermédiaire, c'est-à-dire qu'il serait fait expressément référence à la directive générale de 1995 dans le texte mais que des dispositions plus précises relatives à la protection des données personnelles y seraient également incluses. Quoiqu'il advienne, il est évident que ces dispositions particulières ne seraient que des mesures de précision par rapport à la directive générale, et ne constitueraient aucunement des dérogations aux principes et règles posées par celle-ci.

Bien entendu, la CNIL, comme le groupe de l'article 29, suivra l'évolution de cette proposition de directive. En effet, compte tenu des évolutions de ce texte, il est probable que les discussions à venir feront émerger certains points précis en vue d'une meilleure harmonisation — par exemple, la détermination des durées de conservation des données enregistrées dans la base, les mesures pratiques d'information des personnes sur l'enregistrement de leurs données et leurs droits, etc. À cet égard, le document de travail du groupe sur les listes noires présenté plus haut aura une utilité certaine.

La proposition de directive ouvre par ailleurs une faculté, qui n'a, jusqu'à présent, pas trouvé d'écho favorable de la part du législateur français, et qui consiste à instituer, outre une liste « négative » d'incidents de paiement, une liste « positive ». Ces listes positives recensent, outre les incidents de paiement éventuels que certains débiteurs ont pu occasionner, tous les encours de crédit des personnes ayant demandé un crédit, sans que celles-ci aient fait l'objet de retards de paiement. Ce sujet particulier a fait l'objet d'une étude comparée de la CNIL sur le « *crédit referencing »* aux Etats-Unis, au Royaume-Uni et en Allemagne.

Le débat reste récurrent dans notre pays sur l'opportunité éventuelle de mettre en place de telles listes positives, la proposition de directive présentée ayant partiellement contribué à remettre le sujet à l'ordre du jour.

Chapitre 6

LA CIRCULATION DES DONNÉES DE SANTÉ

Il n'est pas de domaine où la tension soit plus forte que celui de la santé, entre les exigences de la circulation de l'information et celles de protection des données personnelles appelées à circuler. Ces données relèvent en effet de l'intimité de la vie privée. Or, le pilotage du système de santé dans toutes ses composantes, — maîtrise des dépenses de santé, gestion du risque, épidémiologie et veille sanitaire — requiert une connaissance de plus en plus fine, pour ne pas dire personnalisée, de ces données.

En outre notre pays, encore relativement déficient sur le terrain de la prévention et de l'alerte, s'est doté ces dernières années d'instituts, d'agences ou de conseils, qui visent à assurer ce pilotage au niveau central. Non seulement les données médicales circulent mais elles sont de plus en plus centralisées. La CNIL est donc appelée à jouer un rôle de régulateur au bénéfice de personnes qui, hors les syndromes les plus socialement sensibles (sida), ne perçoivent pas nécessairement eux-mêmes spontanément les risques inhérents à cette circulation. Paradoxalement la nouvelle loi sur les droits des malades qui ouvre aux personnes un accès direct à leur dossier médical accroît encore les risques. Demain que restera-t-il du secret médical ?

I. L'IMPERATIF DE SECURITE EN MATIERE DE DONNÉES DE SANTÉ

Aux termes de l'article 29 de la loi du 6 janvier 1978, le responsable d'un traitement doit prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment empêcher qu'elles ne soient communiquées à des tiers

non autorisés. Ces mesures revêtent une importance toute particulière lorsque des données de santé sont traitées.

Le respect de la confidentialité des données médicales peut s'apprécier par l'examen pratique des mesures de sécurité physiques et logiques mises en place mais également par la possibilité, dans certains cas, de recourir à des techniques d'anonymisation des données.

La Commission est particulièrement vigilante à cet égard. Outre les recommandations pratiques qu'elle diffuse à ce sujet (le guide des professions de santé qui comprend un ensemble de fiches destinées à éclairer les professionnels de santé sur l'application de la loi informatique et libertés[1]), elle entend user des pouvoirs de contrôle sur place qui lui sont conférés par la loi pour vérifier ponctuellement l'effectivité des mesures de sécurité mises en place comme l'illustrent les cas suivants.

A. La sécurité informatique à l'hôpital : une nécessaire prise de conscience

La Commission a décidé, par délibération du 15 mai 2001, de procéder à une mission de contrôle sur place auprès de l'hôpital de Mont-Saint-Martin (Meurthe-et-Moselle) géré par l'association hospitalière du bassin de Longwy afin de vérifier l'ensemble des mesures de sécurité mises en œuvre pour garantir la confidentialité des données nominatives conservées au sein du département d'information médicale (DIM).

La CNIL avait en effet été saisie par le Conseil national de l'ordre des médecins d'une plainte faisant état des difficultés rencontrées par un médecin ayant exercé les fonctions de responsable du département d'informations médicales au sein de cet hôpital. Des membres de la direction informatique de l'hôpital auraient accédé, sans autorisation spécifique du médecin DIM, à des informations médicales nominatives relatives à l'activité de certains praticiens de l'établissement conservées dans le serveur placé sous la responsabilité du médecin DIM. Des informations erronées auraient ainsi été introduites dans l'application.

Aux termes de l'article L. 6113-7 du Code de la santé publique, les établissements de santé, publics ou privés, sont tenus de procéder à l'analyse de leur activité (programme de médicalisation des systèmes d'information — PMSI). À cet effet, ils doivent mettre en oeuvre, dans le respect du secret médical et des droits des malades des systèmes d'information qui tiennent compte notamment des pathologies et des modes de prise en charge, en vue d'améliorer la connaissance et l'évaluation de l'activité et des coûts et de favoriser l'optimisation de l'offre de soins.

Pour l'établissement de ces systèmes, le praticien responsable de l'information médicale, qui reçoit des autres praticiens exerçant dans l'établissement les données médicales nominatives nécessaires à l'analyse de leur activité est garant de la qualité des données et doit assurer leur confidentialité.

[1] Disponible sur le site de la CNIL.

En application des articles R. 710-5-4 et suivants du Code de la santé publique, le médecin DIM a une mission de conseil auprès des autres praticiens pour la production des informations. Il veille à la qualité des données qu'il peut confronter, en tant que de besoin, avec les dossiers médicaux et les fichiers administratifs. Il est soumis dans le cadre de ses fonctions de médecin DIM au respect du secret médical et il en est de même des personnels placés ou détachés auprès du médecin DIM et qui travaillent à l'exploitation de données nominatives sous son autorité, ainsi que des personnels intervenant sur le matériel et les logiciels utilisés pour le recueil et le traitement des données.

Il appartient au directeur de l'établissement de prendre toutes dispositions utiles avec le médecin responsable de l'information médicale et après avis de la commission médicale d'établissement afin de préserver la confidentialité des données médicales nominatives. Ces dispositions concernent notamment l'étendue, les modalités d'attribution et le contrôle des autorisations d'accès, ainsi que l'enregistrement des accès.

L'ensemble de ces dispositions semble ne pas avoir été respecté au sein de l'établissement.

Le contrôle de la CNIL a permis de constater que le logiciel, qui permet uniquement en réalité la fourniture des résumés de sortie standardisés pour le PMSI, était un logiciel « maison », conçu à l'origine sans cahier des charges précis, et dont les règles de fonctionnement n'étaient décrites dans aucune documentation écrite officielle de l'hôpital. Aucune remise à niveau du système n'avait été effectuée depuis sa mise en service au début des années 90. Des défauts de conception étant apparus, le service informatique avait ainsi été amené à intervenir progressivement dans le serveur du département d'informations médicales et à dépasser la limite habituellement fixée à l'aide technique et la maintenance informatique.

Par conception, l'application ne prévoyait aucune hiérarchisation des accès. La seule possession du mot de passe dont l'attribution et la gestion n'obéissaient à aucune règle prédéfinie permettait de consulter l'intégralité du dossier. En outre, il est apparu que les mots de passe attribués en 1992 lors de la mise en place du système n'avaient pas été modifiés depuis. Un mot de passe pouvait être commun à plusieurs personnes.

Aucune politique de sécurité n'existait donc au sein de cet établissement. Dès lors, l'état du système informatique et les modalités actuelles de son fonctionnement ne permettaient pas de répondre aux exigences requises en matière de respect de la confidentialité.

C'est pourquoi la CNIL, par délibération du 17 septembre 2002, a décidé d'adresser un avertissement à l'association hospitalière du bassin de Longwy.

Dans la mesure où l'établissement a indiqué se doter prochainement d'un nouveau système informatique, la Commission a demandé à en être saisie dans les plus brefs délais. Elle a également demandé un descriptif précis des mesures de sécurité retenues pour garantir la confidentialité des données, en particulier en ce qui concerne les modalités d'accès aux informations, la politique d'attribution et de composition des mots de passe et les modalités retenues pour assurer une journalisation des connexions.

B. Le respect de l'anonymat : une condition nécessaire à l'établissement de statistiques médicales

La CNIL a mené auprès de la société Cegedim une vérification sur place de l'application Doc'Ware-Thales.

Cette application est une base de données médicales alimentée par des informations télétransmises par un échantillon de médecins, dotés à cet effet par la société Cegedim d'un équipement informatique et d'un logiciel dénommé Doc'ware, leur permettant de gérer leur fichier de patients, d'éditer automatiquement ordonnances, certificats, lettres aux confrères, feuilles de soins, de gérer la comptabilité et de disposer de bases de données sur les médicaments.

Aux termes du contrat liant la société et les médecins se dotant de ce logiciel, ces derniers sont informés que certaines informations anonymes sont communiquées à la société à des fins d'utilisation statistique dans le cadre de diffusion d'études en épidémiologie et en santé publique.

L'objet du contrôle conduit par la CNIL était de vérifier sur place les modalités effectives d'extraction et de télétransmission des informations, ainsi que leurs conditions d'exploitation par la société, afin notamment de s'assurer du caractère anonyme des données relatives aux patients et de la compatibilité du dispositif avec les dispositions de l'article L. 4113-7 du Code de la santé publique qui interdisent *« la constitution et l'utilisation à des fins de prospection ou de promotion commerciale de fichiers composés à partir de données issues directement ou indirectement des prescriptions* [...] dès *lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel de santé ».*

Lors du contrôle, la Commission a pu constater que si les informations télétransmises par le médecin à la société ne permettaient pas en tant que telles d'identifier un patient, l'association de ces données avec un « numéro de patient » attribué par le médecin et inclus dans les traitements d'exploitation mis en œuvre par cette société, ne garantissait pas que l'anonymat du patient soit préservé en toutes circonstances. De surcroît, le fait que la société Cegedim assure la maîtrise totale de l'ensemble des fonctionnalités du logiciel, ainsi que de la procédure d'extraction des données depuis le fichier local du professionnel de santé, a renforcé la nécessité pour la CNIL d'exiger la mise en oeuvre de mesures qui seraient de nature à garantir davantage l'anonymat des patients.

Ainsi, elle a demandé que les données médicales enregistrées dans les fichiers locaux des médecins soient chiffrées et que le dispositif repose sur une clé de cryptage ne devant être connue que du seul médecin.

En outre, elle a considéré que le numéro identifiant le patient qui est enregistré dans la base d'exploitation devait être différent du numéro produit par le poste de travail du médecin. Dès lors, la mise en oeuvre sur le poste de travail du médecin d'une fonction de type « hachage » avec clé secrète, créant un nouveau numéro de patient lors de l'extraction des données, est apparue indispensable.

En ce qui concerne le respect des dispositions de l'article L. 4113.7 du Code de la santé publique, la CNIL a pu constater que le service des études de la société qui est chargé d'établir des tableaux statistiques, en vue d'évaluer l'activité et les prescriptions des médecins, dispose de l'ensemble des informations transmises, ces informations étant associées, non pas à l'identité du médecin concerné, mais à un numéro d'identification du médecin, lequel est cependant utilisé par ailleurs par d'autres services de la société. Un responsable dispose d'une table de correspondance entre ce numéro et l'identité du médecin.

La Commission a considéré que pour assurer le respect des dispositions du Code de la santé publique, la société devait mettre en œuvre un cloisonnement entre la base de données des études statistiques et les autres fichiers, par l'utilisation d'un identifiant spécifique du médecin, propre au service des études statistiques et procéder au chiffrement de la table de correspondance entre le numéro d'identification utilisé par le service des études statistiques et l'identité des médecins concernés. De surcroît, le poste de travail du responsable de cette table de correspondance devait être isolé du réseau interne.

Enfin, la Commission a demandé que toutes mesures soient prises pour permettre aux médecins de visualiser en clair et non sous forme codée les informations télétransmises.

La société Cegedim s'est engagée à prendre en compte ces différentes mesures et, conformément à la demande de la Commission, lui a adressé les éléments techniques de nature à lui permettre de s'assurer que les mesures seront effectivement mises en oeuvre.

II. LA CONSOMMATION MEDICALE À L'ÉTUDE

A. L'enquête décennale sur la santé et la consommation médicale

L'Institut national de la statistique et des études économiques (INSEE) a présenté à la CNIL une demande d'avis concernant la mise en œuvre d'un traitement automatisé d'informations individuelles à l'occasion de l'enquête obligatoire sur la santé et la consommation médicale qui doit se dérouler d'octobre 2002 à septembre 2003.

Depuis 1960, l'INSEE réalise tous les dix ans, auprès d'un échantillon de population, cette enquête santé[1] qui constitue une référence unique sur la mesure de la santé et de la consommation médicale en population générale et dont les résultats sont très attendus notamment par le Haut Comité de santé publique. Toutefois, à la différence des enquêtes précédentes, l'INSEE a souhaité compléter les informations

[1] Cette enquête a fait l'objet de déclarations auprès de la CNIL en 1981 et 1991.

collectées auprès des personnes par des données gérées par la Caisse nationale d'assurance maladie (CNAMTS), ce qui nécessite de recueillir le NIR (numéro d'inscription au répertoire) des personnes enquêtées. C'est la raison pour laquelle, outre le projet d'arrêté portant création du traitement de l'enquête santé, l'INSEE a soumis à la CNIL un projet de décret pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'utilisation du NIR pour permettre l'extraction à partir du système national d'information inter-régimes de l'assurance maladie (SNIIRAM[1]), dans des conditions garantissant l'anonymat des personnes, des données sur le volume et la valeur des prestations annuelles d'assurance maladie relatives aux consommations de soins et de biens médicaux, et ainsi effectuer les comparaisons avec les consommations estimées à partir de l'enquête.

L'enquête santé qui est obligatoire — elle a obtenu le visa du Conseil national de l'information statistique prévu par la loi du 7 juin 1951 —, concerne 16 000 ménages en France métropolitaine tirés au sort dans l'échantillon maître issu du recensement de la population de 1999.

Elle a pour objectifs de décrire l'état de santé de la population enquêtée (morbidité déclarée et indicateurs de santé), d'estimer la consommation annuelle de soins et de prévention à partir d'une part, des déclarations faites par les personnes interrogées et d'autre part, des statistiques agrégées relatives aux prestations d'assurance maladie dont ont bénéficié ces dernières, et enfin d'associer aux états de santé et aux consommations de soins et de prévention, les données socio-démographiques relatives aux individus et aux ménages enquêtés.

L'opération de collecte doit se dérouler sur douze mois. L'enquête réalisée en face à face, prévoit trois visites d'une heure sur deux mois :

— Au cours de la première visite, sont collectées des données sur les caractéristiques socio-démographiques du ménage, le logement, les revenus, la couverture sociale, les handicaps, les gênes et difficultés dans la vie quotidienne. Le questionnaire « individuel » concernant les personnes de plus de 18 ans comporte des questions sur la santé, les maladies en cours, le recours au médecin pendant les douze derniers mois.

— La seconde visite porte sur les nouvelles maladies depuis la dernière visite, les consommations médicales durant la même période, les hospitalisations, les alitements et les interruptions d'activité.

— La troisième visite vise à connaître l'incapacité, les habitudes alimentaires et la prévention. En fin de troisième visite, il est prévu de recueillir, si les personnes interrogées acceptent de le fournir, leur numéro de Sécurité sociale.

[1] Le SNIIRAM a fait l'objet d'un avis favorable de la CNIL (cf. 22° rapport d'activité p. 67, délibération n° 01-054 du 18 octobre 2001)

B. L'utilisation du NIR

Le recueil de ce numéro a pour seul objet de permettre à la CNAMTS, gestionnaire du SNIIRAM, de rechercher dans cette base les enregistrements correspondant aux consommations de soins des personnes enquêtées, dans des conditions garantissant l'anonymat des personnes, afin d'établir des statistiques sur le volume et la valeur des prestations annuelles d'assurance maladie.

À cet effet, l'INSEE doit transmettre à la CNAMTS une liste de NIR cryptés avec le logiciel FOIN (fonction d'occultation d'information nominative) déjà utilisé par la CNAMTS pour anonymiser les données d'identification des bénéficiaires de l'assurance maladie figurant dans le SNIIRAM.

Il convient en effet de rappeler que la CNAMTS a pris des dispositions précises pour garantir l'anonymat des bénéficiaires de soins figurant dans le SNIIRAM, dispositions que la CNIL a examinées avec une particulière attention lors de sa délibération du 18 octobre 2001.

Ainsi, avant toute transmission de données au SNIIRAM, il doit être procédé à l'anonymisation de tous les matricules identifiants, c'est-à-dire au transcodage de ces matricules, selon un dispositif de codage irréversible (recourant à un algorithme dit de « hachage »), en des numéros *non* signifiants mais uniques qui permettent sans réidentification possible de la personne, d'apparier sur un même individu les données relatives aux différentes prestations qui lui ont été servies. Ces numéros font à nouveau l'objet d'une opération de transcodage lors de leur réception par la CNAMTS.

En l'espèce, il est prévu que l'INSEE procède au transcodage des NIR des personnes enquêtées et transmette à la CNAMTS la liste des NIR ainsi transcodés, à charge pour cette dernière de re-transcoder les numéros à partir desquels elle recherchera dans le SNIIRAM les données de consommations correspondant audits numéros. Les données doivent ensuite être restituées à l'INSEE sous forme de statistiques agrégées.

L'INSEE a de plus pris l'engagement de détruire la liste des NIR dès la fin du transcodage.

L'INSEE est le seul destinataire des données recueillies. Le Centre de recherche, d'études et de documentation en économie de la santé (CREDES) doit recevoir un fichier anonymisé avec un numéro d'ordre non signifiant pour procéder au codage des maladies et des consommations déclarées lors de l'enquête. Après codage, le fichier sera retourné à L'INSEE.

Il est également prévu que la DREES (service statistique du ministère des Affaires sociales) obtiendra un fichier anonymisé comportant les codes communes afin de coder le secteur sanitaire.

Compte tenu des précautions prises en l'espèce tant par l'INSEE que par la CNAMTS, la Commission a émis un avis favorable au projet de décret, pris en application de l'article 18 de la loi du 6 janvier 1978, visant à autoriser l'INSEE à utiliser le NIR collecté, de manière facultative, lors de l'enquête santé, sous réserve qu'il

comporte le contreseing du ministre des Affaires sociales, du Travail et de la Solidarité, et au projet d'arrêté portant création du traitement automatisé d'informations individuelles concernant l'enquête santé.

III. LE RENFORCEMENT DE LA VEILLE SANITAIRE

A. Les conditions d'accès aux données de santé en cas d'urgence sanitaire

L'Institut de veille sanitaire (InVS) est chargé, conformément aux dispositions de l'article L. 1413-2 du Code de la santé publique, d'effectuer la surveillance et l'observation permanente de l'état de santé de la population, d'alerter les pouvoirs publics, notamment les agences sanitaires, en cas de menace pour la santé publique, quelle qu'en soit l'origine, et de leur recommander toute mesure ou action appropriées. Il lui appartient également de mener toute action nécessaire pour identifier les causes d'une modification de l'état de santé de la population, notamment en situation d'urgence.

Dans ce cadre, l'article L. 1413-5 du Code de la santé publique dispose qu'« à *la demande de l'Institut de veille sanitaire, lorsqu'il s'avère nécessaire de prévenir ou de maîtriser des risques pour la santé humaine, toute personne physique ou morale est tenue de lui communiquer toute information en sa possession relative à de tels risques. L'Institut accède, à sa demande, aux informations couvertes par le secret médical ou industriel dans des conditions préservant la confidentialité de ces données à l'égard des tiers ».*

La CNIL a été consultée sur le projet de décret en Conseil d'État appelé à fixer les conditions dans lesquelles l'InVS accède à ces informations (délibération n° 02-021 du 2 avril 2002). Le texte reconnaît ainsi à l'InVS la possibilité d'accéder rapidement aux données, et ce sans opposition possible de la personne concernée, du professionnel de santé détenteur des données ou de l'entreprise dès lors qu'il s'agit de déterminer les causes de telle ou telle épidémie ou d'exposition à un risque physique, chimique ou biologique et de prendre le plus rapidement possible les mesures efficaces de santé publique qui s'imposent pour l'enrayer.

La qualité de tiers autorisé au sens de la loi du 6 janvier 1978 est donc reconnue par la loi à l'InVS. Les conditions de communication des données telles que précisées dans le projet de décret s'inscrivent dans le droit fil des critères retenus par la CNIL pour qualifier une personne physique ou morale de tiers autorisé.

Il est ainsi prévu que toute communication d'information à l'Institut de veille sanitaire fera l'objet d'une demande écrite et motivée de sa part. La demande ainsi formulée devra mentionner le nom ainsi que l'adresse administrative et électronique de la personne à laquelle ces informations seront transmises. Seul un professionnel de santé pourra être désigné s'il s'agit d'informations de nature médicale. La

demande devra également mentionner la durée prévisible de conservation de ces informations. Il est en outre prévu que la demande soit satisfaite sans délai, dans des conditions permettant d'en garantir la confidentialité. Ainsi lorsque ces informations seront transmises par voie postale, elles devront être adressées sous double enveloppe, celle placée à l'intérieur devant porter la mention « secret médical » ou « secret industriel ».

La possibilité d'une transmission par voie électronique de ces informations est prévue. Sur ce point, la Commission a estimé que les données ainsi télétransmises devront faire l'objet d'un chiffrement.

B. La surveillance des maladies à déclaration obligatoire

1. LE CADRE LÉGAL ET RÉGLEMENTAIRE

Le cadre juridique de la surveillance épidémiologique des maladies à déclaration obligatoire est défini par la loi du 1er juillet 1998 sur la veille sanitaire. L'article L. 3113-1 du Code de la santé publique dispose que les maladies qui nécessitent une intervention urgente, locale, nationale ou internationale et les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique font l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire.

En outre, la loi prévoit que les modalités de transmission des données et, en particulier la manière dont l'anonymat est protégé, sont fixées par décret en Conseil d'État.

Depuis 1999, la CNIL a déjà eu à connaître à plusieurs reprises des nouvelles modalités de mise en oeuvre de cette surveillance, tout particulièrement, à la suite de la décision prise par le ministre de la Santé en 1998 d'inscrire la séropositivité au VIH parmi la liste des maladies à déclaration obligatoire *[cf.* rapports annuels 2000 et 2001).

La Commission a en outre été saisie en octobre 2002 par l'InVS, conformément aux dispositions du chapitre Vbis de la loi du 6 janvier 1978, d'une demande d'autorisation concernant l'application informatique destinée à gérer la surveillance épidémiologique des maladies infectieuses à déclaration obligatoire. La liste de ces maladies, au nombre de vingt-six, est fixée par l'article D. 11-1 du Code de la santé publique.

De façon concomitante, la CNIL a également été saisie par le directeur général de la santé d'un projet d'arrêté relatif à la notification obligatoire des maladies, pris en application des dispositions du décret du 16 mai 2001 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire.

Aux termes de ce texte, codifié aux articles R. 11-2 et suivants du Code de la santé publique, il est en effet prévu que pour chaque maladie à déclaration obligatoire, un arrêté du ministre chargé de la Santé, pris après avis de la Commission

nationale de l'informatique et des libertés, fixe, pour chaque maladie, les informations destinées à la surveillance épidémiologique et, en particulier, les données cliniques, biologiques et socio-démographiques que le médecin déclarant ou, en cas de diagnostic biologique, le médecin prescripteur porte sur la fiche de notification.

2. LE CONTENU DES FICHES DE NOTIFICATION

Dans un souci de simplification, la CNIL s'est prononcée par délibération n° 02-082 du 19 novembre 2002 sur un seul projet d'arrêté relatif à la notification obligatoire des maladies infectieuses visées à l'article D. 11-1 du Code de la santé publique auquel sont annexés les modèles de fiche des maladies, englobant donc également la fiche relative à la notification obligatoire de l'infection aiguë symptomatique par le virus de l'hépatite B et de l'infection par le virus de l'immunodéficience humaine, quel que soit le stade sur laquelle la Commission s'était déjà prononcée spécifiquement le 21 mars 2002 (délibération n° 02-020 du 21 mars 2002).

Pour toutes les maladies, outre les données relatives au professionnel de santé déclarant et au code d'anonymat, sont recueillies des données cliniques, biologiques et socio-démographiques, variables en fonction des maladies, mais qui concernent principalement la date des premiers signes cliniques de la maladie, la date et le lieu d'hospitalisation, les signes cliniques et les résultats biologiques permettant de déterminer si les critères de déclaration sont remplis, l'évolution de la maladie, les facteurs de risque, les antécédents de prophylaxie et les éléments permettant de déterminer une exposition ou le mode de transmission. Dans certains cas, des données concernant les mesures de prophylaxie mises en œuvre dans l'entourage ou la communauté seront recueillies.

La CNIL a considéré que le formulaire de déclaration des cas d'infections par le virus de l'immunodéficience humaine devait être modifié de façon à supprimer l'indication de la mention relative à la nationalité de naissance ainsi que la référence au service militaire. Elle a en effet estimé que les données relatives au pays de naissance, au pays de domicile et à la nationalité actuelle constituent des indicateurs suffisants et que l'information relative à la nationalité à la naissance, outre le fait qu'il n'entre pas dans l'exercice habituel de l'activité professionnelle des médecins de recueillir cette information sous une forme aussi détaillée, apparaissait excessive au regard de la finalité poursuivie.

La Commission a également estimé que le recueil, sous une forme détaillée de la profession, ne pouvait être admis que dans la mesure où la confidentialité des déclarations lors de leur transmission aux DDASS et à l'InVS serait parfaitement assurée et où il serait procédé lors de la saisie informatique par l'InVS des déclarations à la codification de cette information selon une nomenclature de catégories socioprofessionnelles évitant tout risque de réidentification.

Sur les variables biologiques qui sont relatives aux sérologies antérieures négatives et positives, au nombre total de sérologies réalisées, à la date de prélèvement, au type de virus et au profil de séroconversion, la Commission n'a pas émis

d'observation particulière. Ces données sont complétées d'informations sur le ou les motifs de dépistage et le stade clinique de l'infection.

Le mode et la date de contamination probable, variables fondamentales pour la surveillance de l'infection VIH, sont collectés, de même que des informations sur la nature des rapports sexuels et l'usage de drogues injectables.

Le formulaire comporte également une rubrique sur le partenaire à l'origine probable de la contamination. Il est ainsi demandé si le partenaire vit ou a vécu dans une communauté où la prévalence est élevée (Afrique sub-saharienne, Caraïbes, Asie du sud et du sud-est, autre). Cette information permet de caractériser le mode de contamination.

La Commission a pris acte que la collecte de ces informations était justifiée par la nécessité d'une part, de déterminer si les partenaires ont vécu ou séjourné dans des pays qui connaissent une forte épidémie de sida et où la transmission hétérosexuelle du virus est actuellement prédominante et d'autre part, de pouvoir définir ainsi l'origine du virus, dans la mesure où il peut exister des types de virus différents selon les zones géographiques.

3. LES GARANTIES D'ANONYMAT

La procédure d'anonymisation retenue par l'InVS est réalisée par l'utilisation d'un logiciel de hachage qui permet de générer, à partir de la première lettre du nom de la personne, de son prénom, de sa date de naissance et de son sexe, un numéro d'anonymat sous forme d'une chaîne de seize caractères, numéro qui sera porté de façon manuscrite sur la fiche de notification du cas.

Il est prévu une première anonymisation au niveau local, réalisée soit par les laboratoires pour les infections VIH et VHB, par les médecins hospitaliers pour le sida, les infections à VIH, soit par les médecins inspecteurs de santé publique des directions départementales des affaires sanitaires et sociales pour les autres maladies à déclaration obligatoire. Ces dernières (à l'exclusion du VIH/sida et de l'hépatite B) nécessitent en effet, conformément aux dispositions de l'article L. 3113-1 du Code de la santé publique, une intervention urgente locale, nationale ou internationale. Dès lors, le choix retenu de ne procéder à l'anonymisation qu'au niveau de la DDASS résulte du fait que ces maladies doivent faire l'objet d'un signalement immédiat non anonymisé à la DDASS, afin de permettre la conduite d'investigations pour identifier l'origine de la contamination et la mise en place rapide de mesures de prévention individuelle et collective.

Une fois la fiche de notification transmise à l'InVS, celui-ci procédera à une seconde anonymisation, à partir du résultat de la première anonymisation et d'une clé secrète détenue par lui.

Cette technique de double anonymisation, préconisée par la CNIL dans les cas les plus sensibles et évaluée, à la demande de la Commission, en 1996 et 1997 par le service central de sécurité des systèmes d'information, est déjà mise en œuvre pour le chaînage des données dans le cadre du programme de médicalisation des

systèmes d'information et pour certaines enquêtes dans le domaine social (observatoire du RMI). C'est également la technique retenue pour le système national d'information interrégimes de l'assurance maladie (SNIIRAM) mis en place par la CNAMTS. Le calcul de ce numéro fait appel à un algorithme de « hachage » permettant de transformer de façon non réversible des éléments d'identification en un numéro anonyme et unique, sans réidentification possible du patient tout en permettant d'apparier sur un même individu les données recueillies successivement.

La double anonymisation a pour but de couper tout lien entre le patient et les données le concernant, dans les deux sens : d'une part les personnels de l'InVS ne peuvent connaître l'identité des patients dont les fiches ne lui sont adressées que sous le premier code d'anonymat et, d'autre part, les déclarants ou les médecins inspecteurs des directions départementales des affaires sanitaires et sociales ne peuvent re-identifier le contenu de la base de données qui utilise un deuxième code d'anonymat pour l'enregistrement des données.

4. LE RESPECT DES DROITS DES PERSONNES

Sur l'information des personnes concernées, l'InVS a proposé d'élaborer une note individuelle destinée à informer clairement la personne sur le principe de la déclaration obligatoire. Un dépliant d'information sera ainsi remis à chaque personne concernée. De même, tous les professionnels de santé concernés seront destinataires d'une information très complète de l'InVS sur la mise en place du nouveau dispositif et sur le rôle qu'ils ont à jouer pour garantir le bon fonctionnement de cette surveillance épidémiologique.

Le droit d'accès aux informations s'exercera auprès de l'InVS par l'intermédiaire du médecin qui a procédé à la notification et uniquement pendant un délai de six mois après que le médecin a transmis la fiche. En effet, à l'issue de ce délai, les informations concernant le patient dans la base de données sont rendues non identifiantes par la suppression des tables de correspondance.

Compte tenu des garanties prises, la CNIL a autorisé l'Institut national de veille sanitaire à mettre en place le système de surveillance des maladies à déclaration obligatoire.

C. La lutte contre le dopage

La Commission a été saisie pour avis, par le ministère de la Jeunesse et des Sports d'un projet de décret prévu en application des dispositions de l'article L. 3622-7 du Code de la santé publique issues de la loi du 23 mars 1999 relative à la protection de la santé des sportifs et à la lutte contre le dopage. Ce texte a notamment pour objet de déterminer les modalités de transmission aux autorités sanitaires de données individuelles recueillies par les médecins qui traitent des cas de dopage ou de pathologies consécutives à des pratiques de dopage, ainsi que les garanties du respect de l'anonymat des personnes.

1. UN SUIVI INDIVIDUEL DES SPORTIFS

La loi fait désormais obligation à tout médecin qui décèle chez un sportif des signes évoquant une pratique de dopage de refuser la délivrance de certificats médicaux, d'informer son patient des risques encourus du fait de cette pratique et du suivi médical dont il peut bénéficier, de transmettre obligatoirement au médecin responsable d'une antenne médicale spécialisée dans le dopage, sous forme nominative, les constatations faites et d'en informer son patient.

Cette surveillance médicale s'accompagne également d'un dispositif de recueil et de transmission à des fins épidémiologiques de données individuelles qui permettra d'évaluer l'état du dopage en France et d'orienter plus efficacement les politiques de santé et d'éducation.

Le projet de décret a pour objet de décrire les modalités de la transmission des informations individuelles et les mesures retenues pour garantir l'anonymat des personnes concernées en reprenant un dispositif analogue à celui défini par les pouvoirs publics pour fixer les modalités de transmission à l'autorité sanitaire des maladies à déclaration obligatoire *(cf. supra)*.

C'est une cellule scientifique de coordination de la recherche fondamentale et appliquée dans les domaines de la médecine sportive et du dopage, composée en particulier de personnes spécialisées en toxicologie et pharmacologie et placée auprès du Conseil de prévention et de lutte contre le dopage, autorité administrative indépendante, qui sera destinataire des données individuelles. Elles lui seront transmises par l'intermédiaire des médecins responsables des antennes médicales de lutte contre le dopage qui, implantées dans des établissements publics de santé, sont placées sous la responsabilité d'un médecin ayant une pratique en pharmacologie, toxicologie ou dans la prise en charge des dépendances.

2. UN DOSSIER ANONYMISÉ

Le projet de décret prévoit qu'une fiche de déclaration sera établie par le médecin responsable de l'antenne médicale de lutte contre le dopage à partir des informations transmises par le médecin traitant. Elle comportera les coordonnées de l'antenne médicale et de son médecin responsable, les coordonnées du médecin traitant et notamment son nom, son prénom et son adresse, les coordonnées d'un autre prescripteur ou d'une tierce personne à l'origine de l'orientation de la personne vers l'antenne médicale. Elle comportera également un numéro d'anonymat établi par codage informatique irréversible à partir des trois premières lettres du nom, du prénom et de la date de naissance et du sexe de la personne.

Il est également prévu que *« le médecin responsable de l'antenne médicale de lutte contre le dopage qui établit la correspondance entre le numéro d'anonymat et les éléments d'identité de la personne en assure la conservation, aux fins de validation et d'exercice du droit d'accès, dans des conditions garantissant la confidentialité des informations et la détruit six mois après la date d'envoi des données à la cellule scientifique du conseil de prévention et de lutte contre le dopage. »*

Ce système est analogue au dispositif d'anonymisation recommandé par la CNIL dans son rapport du 9 décembre 1999 relatif aux modalités d'informatisation de la surveillance épidémiologique du sida et à celui qui a été retenu par le décret du 16 mai 2001 fixant les modalités de transmission à l'autorité sanitaire de donnés individuelles concernant les maladies à déclaration obligatoire. Il permet ainsi à l'aide d'une technique faisant appel à un algorithme de « hachage » de transformer de façon non réversible les données nominatives en un numéro anonyme et unique permettant, sans qu'il soit possible d'identifier la personne, d'apparier cependant sur un même individu les données qui lui sont propres.

Le médecin responsable de l'antenne médicale de lutte contre le dopage transmettra alors la fiche qu'il aura établie accompagnée du numéro d'anonymat établi par codage informatique soit par voie postale sous pli confidentiel portant la mention secret médical, soit par télétransmission après chiffrement des données au médecin responsable de la cellule scientifique du Conseil de prévention et de lutte contre le dopage qui, selon les mêmes modalités, les transmettra à l'InVS chargé, conformément aux dispositions de l'article L. 141 3-2 du Code de la santé publique, de l'observation permanente de l'état de santé de la population.

IV. L'ACCES DES PERSONNES À LEURS DONNÉES DE SANTÉ

A. L'accès au dossier médical : de nouvelles règles

Les services de la CNIL ont élaboré un *Guide des professions de santé*[1] , comportant plusieurs fiches thématiques, dont l'une est consacrée à « l'accès au dossier médical ». Cette fiche comporte des informations pratiques sur les modalités d'accès aux données personnelles de santé.

En effet la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a posé le principe de l'accès direct du patient à l'ensemble des informations de santé le concernant, et le décret du 29 avril 2002[2] a organisé cet accès. Néanmoins le patient peut toujours, s'il le souhaite, accéder à ces données par l'intermédiaire d'un médecin de son choix.

La communication doit être faite au plus tard dans les huit jours suivant la demande et au plus tôt dans les quarante-huit heures. Si les informations remontent à plus de cinq ans, le délai est porté à deux mois. Cette période de cinq ans court à compter de la date à laquelle l'information médicale a été constituée.

[1] Ce guide, disponible sur le site www.cnil.fr, au chapitre « dossiers thématiques », dans la rubrique « san té ».

[2] Décret n° 2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les pro fessionnels et établissements de santé en application des articles L. 1111-7 et L. 1112-1 du Code de la santé publique.

La présence d'une tierce personne peut être recommandée par le médecin mais ne peut empêcher un accès direct au dossier en cas de refus du patient de suivre cette recommandation.

1. QUI PEUT DEMANDER L'ACCES AU DOSSIER MEDICAL ?

L'accès au dossier médical peut être demandé auprès du professionnel de santé ou de l'établissement de santé, par la personne concernée, son ayant droit en cas de décès de cette personne, le titulaire de l'autorité parentale, le tuteur ou le médecin désigné comme intermédiaire.

2. QUELLES SONT LES INFORMATIONS COMMUNICABLES ?

Toute personne a accès à l'ensemble des informations concernant sa santé, c'est-à-dire à toutes les données qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment les résultats d'examen, les comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, les protocoles et prescriptions thérapeutiques mis en oeuvre, les feuilles de surveillance, les correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers[1].

Ces informations sont communicables qu'elles soient sous forme papier ou sur support informatique. La communication, en langage clair (par exemple, par l'indication de la signification des codes utilisés), doit être conforme au contenu des enregistrements.

3. QUELLES SONT LES MODALITES D'ACCES ET DE COMMUNICATION ?

La demande est adressée au professionnel de santé ou au responsable de l'établissement ou à la personne désignée à cet effet par ce dernier.

L'accès aux données se fait, au choix du demandeur, soit par consultation sur place avec éventuellement remise de copies, soit par l'envoi des documents (si possible en recommandé avec accusé de réception). Les frais de délivrance de ces copies sont à la charge du demandeur et ne sauraient excéder le coût de la reproduction et, le cas échéant, de l'envoi des documents.

Préalablement à toute communication, le destinataire de la demande doit vérifier l'identité du demandeur (ou la qualité de médecin de la personne désignée comme intermédiaire).

[1] Article L. 1111-7 du Code de la santé publique ; voir également l'article R. 710-2-2 du Code de la santé publique relatif au contenu du dossier médical.

En cas de refus ou d'absence de réponse du professionnel ou de l'établissement de santé, le demandeur peut saisir la CNIL.

B. Les plaintes concernant l'accès aux données personnelles de santé

Depuis l'entrée en vigueur des dispositions de la loi du 4 mars 2002 et de son décret d'application, posant le principe de l'accès désormais direct aux données personnelles de santé, le nombre de plaintes de patients rencontrant des difficultés pour obtenir l'accès à des données médicales a nettement diminué.

1. DES CAS UN PEU PARTICULIERS

Ces plaintes se rapportent essentiellement à des cas particuliers.

Tel est le cas de M. C. qui souhaite accéder aux données de santé concernant son frère, dont il est le tuteur, ainsi qu'à celles concernant ses parents, détenues par des établissements hospitaliers.

La Commission a informé M. C. qu'il pouvait demander l'accès aux données médicales de son frère puisqu'il est son tuteur. En revanche, il ne peut accéder aux informations concernant ses parents qui devront, s'ils le souhaitent, accomplir eux-mêmes, individuellement, les démarches.

M. J. a saisi la CNIL car un hôpital lui a refusé l'accès au dossier médical de son père décédé.

Dans ce cas, la Commission a rappelé à M. J. les dispositions particulières de l'article L. 1 110-4 du Code de la santé publique. Ainsi, M. J. doit préciser, lors de sa demande à l'établissement hospitalier, le motif pour lequel il a besoin d'avoir connaissance de ces informations (permettre de mieux connaître les causes de la mort, défendre sa mémoire, faire valoir des droits). Cependant, M. J. ne pourra avoir communication du dossier si son père a exprimé une volonté contraire avant son décès.

2. LA RECTIFICATION DU DOSSIER MÉDICAL

La CNIL a par ailleurs été saisie de plaintes qui se rapportent aux difficultés que peuvent rencontrer des patients à exercer leur droit de rectification aux données de santé, après y avoir accédé.

Le cas de M^{me} B. illustre bien les situations, souvent délicates, dans lesquelles peuvent se trouver tant les patients que les professionnels de santé,

M^{me} B est suivie par un médecin d'un cabinet médical. Son médecin habituel étant absent, elle est reçue par un autre praticien.

Elle découvre, lors de cette visite, qu'un commentaire indiquant *« patiente à tendance suicidaire »* figure dans sa fiche. M^{me} B. souhaite que ce commentaire, dont son médecin habituel est à l'origine, ne figure plus dans ce fichier.

N'obtenant pas satisfaction, elle saisit la CNIL.

D'un point de vue juridique, M^me^ B. peut invoquer, à l'appui de sa demande, soit les dispositions de l'article 36 de la loi du 6 janvier 1978, soit celles de son article 26 alinéa 1.

L'article 36 dispose en effet que *« le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte et l'utilisation, la communication ou la conservation est interdite ».*

L'article 26 alinéa 1 de la loi du 6 janvier 1978 prévoit par ailleurs que toute personne physique peut s'opposer, pour des raisons légitimes, à ce que des informations la concernant fassent l'objet d'un fichier.

La notion de « raisons légitimes » n'est pas définie par la loi, et il appartient en dernier recours aux juridictions compétentes d'apprécier la légitimité des motifs invoqués par une personne pour demander la radiation d'un fichier de données la concernant.

L'application de ces dispositions aux données médicales est particulièrement délicate. Une concertation entre le patient et son médecin, dans le cadre d'un colloque singulier, à l'occasion de laquelle le patient pourra expliquer et motiver clairement les raisons pour lesquelles il souhaite faire rectifier ou supprimer les données médicales le concernant, semble indispensable.

En cette matière, le rôle de la CNIL consiste principalement à « provoquer » une telle concertation.

Dans le cas de M^me^ B., le souci de préserver la relation de confiance avec sa patiente a conduit son médecin, à l'occasion de cette concertation, à supprimer le commentaire qu'il avait enregistré dans le fichier médical des patients du cabinet.

3. LES COMPAGNIES D'ASSURANCE

Enfin, la CNIL a reçu des plaintes concernant l'accès aux données médicales détenues par les compagnies d'assurance.

Trop souvent, les plaignants ne peuvent avoir accès à leurs données qu'au terme d'un long parcours, imposé par les compagnies d'assurances.

Le cas de M. P. en est une illustration.

M. P. est victime d'un accident de la circulation au mois de mai 2000. Sa compagnie d'assurance professionnelle lui demande de se faire examiner par un de ses médecins conseils qui établit trois rapports médicaux.

M. P. qui souhaite avoir accès à ces rapports médicaux se heurte à un refus au motif que *« les rapports du Dr. X. sont des documents internes à notre société dont nous ne pouvons nous dessaisir ».*

M. P., après plusieurs tentatives restées vaines, doit saisir la CNIL pour obtenir, enfin, au terme d'une année de démarches, l'accès aux données de santé le concernant.

Chapitre 7

GISEMENTS D'INFORMATIONS À SURVEILLER

L'annuaire universel de tous les abonnés du téléphone, comprenant les coordonnées des 38 millions de détenteurs de mobiles.

La base des images de tous les immeubles des principales villes françaises.

Le fichier des adresses de toutes les familles qui ont récemment déménagé (3 millions par an).

Le recensement : 20 millions de foyers sur le territoire national, y compris les sans abri, les gens du voyage et les mariniers.

La banque de données des salaires déclarés aux organismes de Sécurité sociale.

La simple énumération de ces fichiers montre l'ampleur et la valeur de ces « silos » d'informations administratives. Qu'il s'agisse de projets ou de réalisations bien avancées, la CNIL s'y est intéressée de près en 2002.

I. LES ANNUAIRES DE TÉLÉCOMMUNICATIONS

A. L'annuaire universel

La CNIL a été saisie pour avis d'un projet de décret relatif à l'annuaire universel modifiant le Code des postes et télécommunications. L'avis de la Commission avait déjà été sollicité sur un projet similaire en 1996. Cependant, le décret en question n'a jamais été publié, compte tenu des difficultés de mise en œuvre de l'orga-

nisme *ad hoc* exigé par la loi du 26 juillet 1996 de réglementation des télécommunications. On peut rappeler qu'un annuaire universel regroupe, sous la forme d'un document papier ou électronique, les coordonnées de l'ensemble des abonnés au réseau téléphonique public, quel que soit leur opérateur.

Le projet de décret consacre le droit pour tout abonné de figurer sur une liste d'abonnés ou d'utilisateurs. Chaque opérateur doit tenir la liste de ses abonnés et la communiquer aux fins d'établissement d'un annuaire universel ou de mise en place d'un service de renseignements téléphoniques universel dans des conditions assurant la libre concurrence dans ces secteurs. Il prévoit, par ailleurs, que France Télécom doit éditer un annuaire universel sous forme imprimée et électronique et fournir un service universel de renseignements.

C'est dans ce nouveau cadre que la Commission a examiné le projet qui lui a été soumis.

1. LA SPECIFICITE DE LA TELEPHONIE MOBILE

En premier lieu, la CNIL a relevé la spécificité de la téléphonie mobile et en a tiré une conséquence majeure. En effet, le projet de décret impose aux opérateurs de téléphonie mobile et à leurs distributeurs d'informer leurs abonnés sur « leur droit » à figurer dans les listes d'abonnés et sur les droits qui s'y rattachent. Les abonnés concernés disposent alors d'un délai de six mois à compter de la réception de ladite information pour faire part de leur refus de figurer sur ces listes. À défaut, ils seront réputés avoir consenti à y être mentionnés. En revanche, les utilisateurs des cartes prépayées ne figureront sur les listes d'abonnés qu'à leur demande.

Prenant en compte les conséquences pratiques pour les personnes inattentives ou qui n'auront pas réagi à temps — à savoir, l'inscription dans l'annuaire des numéros de téléphone et de l'adresse des personnes et la possibilité d'être prospectées — et la particularité de la téléphonie mobile — il y a aujourd'hui en France trente-huit millions de personnes abonnées à la téléphonie mobile qui savent, lorsqu'elles s'abonnent, qu'il n'y a pas d'annuaire et ont coutume de n'être appelées que par des personnes auxquelles elles auront volontairement communiqué leur numéro —, la Commission a estimé qu'il serait plus sage et plus conforme à l'esprit de protection des données personnelles et de la vie privée que seules les personnes qui en auraient manifesté expressément la volonté puissent être inscrites dans un annuaire et voir ainsi leur numéro de téléphone communiqué par un service de renseignement.

2. UNE GAMME COMPLEXE MAIS NECESSAIRE DE DROITS

Le projet de décret introduit la gratuité de la liste « chamois » (liste des abonnés qui ne souhaitent pas paraître dans les annuaires) et laisse payante l'inscription en liste rouge (abonnés qui s'opposent, de plus, à ce que leurs coordonnées soient communiquées par les services de renseignements universels). La Commission a réaffirmé sa position constante en faveur de la gratuité de la liste

rouge qui présente le double avantage de tendre à une simplification pour les abonnés de l'exercice de leurs droits d'opposition et de permettre la gratuité de l'exercice de ces derniers.

La Commission se félicite, par ailleurs, de la meilleure protection offerte aux abonnés ayant exercé leur droit d'opposition à être prospectés. D'une part, les abonnés inscrits en liste orange seront désormais identifiables par l'instauration d'un signe distinctif permettant de les identifier dans les annuaires. D'autre part, l'instauration d'une amende prévue pour les contraventions de la cinquième classe pour chaque prospection effectuée par télécopie ou par automates d'appels en infraction avec les dispositions des ordonnances de juillet et août 2001 sera de nature à garantir une meilleure effectivité du droit d'opposition. On doit cependant noter, sur ce point, que le projet de loi relatif à la confiance dans l'économie numérique, en modifiant la rédaction de l'article L. 33-4-1 du Code des postes et télécommunications, reprend le principe du consentement préalable en matière de prospection directe opérée, notamment, par voie d'automates d'appel et de télécopieurs. Il est donc probable que les sanctions pénales destinées à réprimer l'inobservation de ce principe soient prévues, non pas dans le cadre du décret relatif à l'annuaire universel, mais dans le cadre — plus général — du décret en Conseil d'État devant préciser les conditions d'application de cet article.

La Commission a noté avec satisfaction que l'abonné peut demander que son adresse ne figure pas dans son intégralité dans l'annuaire et qu'il ne soit pas fait référence à son sexe, ce qui signifie en pratique que le prénom pourra être limité à l'initiale. Elle a cependant attiré l'attention des rédacteurs sur la question des possibles contradictions entre les droits retenus par les abonnés auprès des différents opérateurs dont ils seraient clients, en proposant d'appliquer le régime le plus favorable à la protection de la vie privée de l'abonné ou de l'utilisateur.

Afin de compléter ces droits, la Commission a rappelé son souhait que soit consacré le droit de s'opposer à faire l'objet d'une recherche à partir du numéro d'appel et, plus généralement, à figurer dans un annuaire inversé. En pratique, France Télécom avait, dès 1997, pris en compte cette demande en créant l'actuelle liste d'opposition « anti quidonc ». La Commission, prenant en compte les dangers d'utilisation malveillante de tels annuaires, a recommandé d'encadrer leur utilisation par une généralisation et une consécration réglementaire de la pratique observée par France Télécom.

Enfin, afin de garantir un exercice optimal des différents droits reconnus aux abonnés, la Commission a recommandé que le projet de décret relatif à l'annuaire universel impose une information claire des abonnés quant à leurs droits en matière de téléphonie. En effet, si la multiplication des listes d'opposition permet d'affiner, au mieux, le niveau de protection souhaité, elle n'en entraîne pas moins une complexité redoutable pour l'abonné. En conséquence, une solution pourrait être trouvée dans un énoncé préalable et clair des multiples options offertes et ce, dès l'abonnement.

3. QUELS ACCES POUR L'ETAT ?

En troisième lieu, la Commission s'est attachée à ce que soit définie précisément la question de l'accès à la liste universelle par certains services de l'Etat. Tout en considérant que les services d'urgence et de sauvegarde de la vie humaine (SAMU, pompiers, police-secours) étaient fondés à accéder à l'intégralité des données issues de la liste universelle pour l'exercice de leurs missions, elle a préconisé une écriture plus précise de ces dispositions, afin d'en préciser les bénéficiaires et la finalité qui doit être limitée aux fins exclusives d'identification de la personne appelante et de la connaissance de son adresse.

À ce jour, ce décret n'a toujours pas été publié.

B. Des pages jaunes aux photos de résidences privées...

La Commission a été saisie, au cours de l'année 2002, d'un nombre important de réclamations concernant la diffusion sur internet de photos d'immeubles et de maisons individuelles des principales villes françaises. Ces photos sont accessibles sur le site « Les photos de villes », présenté sur le portail « Voilà » ou accessibles à partir du site des pages jaunes/blanches de France Télécom.

1. LA COMPETENCE DE LA CNIL

À partir d'une adresse — aussi bien celle d'un commerçant que d'un particulier — il est possible de voir l'immeuble correspondant. Le site permet ensuite de visualiser les immeubles adjacents puis de se déplacer aisément dans les rues environnantes. Le site permet toujours de rattacher une adresse à un immeuble.

Les plaignants arguent du fait que la diffusion sur internet de la photo de leur maison et de leur immeuble constitue une atteinte à leur vie privée et s'inquiètent, par ailleurs, de l'utilisation frauduleuse qui pourrait être faite de tels renseignements. Ainsi, un plaignant a été fréquemment démarché par des vendeurs de véranda, sa maison n'en possédant manifestement pas. On pourrait aussi soulever la question du droit sur l'image du propriétaire ou celle du droit d'auteur de l'architecte mais la Commission s'est limitée à apprécier l'applicabilité des dispositions de la loi du 6 janvier 1978 à ce service.

En tant que telle, une photo d'immeuble ne constitue pas une donnée nominative. En revanche, cette même photo, associée à l'adresse correspondante, est susceptible de constituer une donnée indirectement nominative. En effet, avec l'utilisation des pages blanches sur internet comme annuaire inversé, il est possible, à partir de la seule adresse, de rattacher — hors cas de liste rouge — un nom de particulier à une photo d'immeuble. Que la photographie de la propriété corresponde à un immeuble comportant plusieurs logements ou à une maison individuelle, elle constitue une donnée indirectement nominative.

À ce titre, et conformément à l'article 16 de la loi du 6 janvier 1978, une déclaration de traitement automatisé d'informations nominatives a été déposée auprès de la CNIL par la filiale de France Télécom éditrice du service « Pages Jaunes ».

2. LE DROIT D'OPPOSITION

Le principal motif de saisine des auteurs de plaintes résidait dans l'exercice de leur droit d'opposition à voir la photo de leur habitation figurer sur le réseau internet. Suite à l'intervention de la Commission, et conformément à l'article 26 de la loi du 6 janvier 1978, un droit d'opposition à figurer dans ce traitement a été reconnu aux personnes. Celui-ci est précisé sous la rubrique « Protection des données » accessible depuis les pages d'accueil du site.

Ce droit d'opposition ne peut cependant s'appliquer que dans le cas d'occupation par une seule et même personne d'un bien immobilier. En effet, au regard de la loi « Informatique et libertés », le droit d'opposition permet à une personne physique (le résident) de s'opposer à ce que des informations nominatives le concernant (l'adresse rattachée à la photo de sa résidence) fassent l'objet d'un traitement. Dès lors, ne peuvent être exclues du traitement que les photos d'immeuble dont l'adresse ne correspond qu'à une seule personne.

De plus, seule la personne dont le nom est rattaché à l'adresse peut exercer ce droit. Ainsi, la possibilité offerte par la loi du 6 janvier 1978 d'enlever la photo d'une maison de la base de données gérée par « Pages Jaunes » n'est pas liée à la qualité de propriétaire du bien concerné, mais à celle d'occupant du lieu (qu'il soit locataire ou propriétaire).

L'exercice de ce droit permet de retirer du traitement l'image de la maison concernée et permet, en toute logique, à un occupant de s'opposer à ce que sa maison soit photographiée par l'équipe de photographes chargés de numériser l'ensemble d'une ville. Il est à noter que France Télécom ne prévoit aucune réactualisation de la liste des maisons qui n'apparaissent pas sur ce site, quand bien même l'occupant changerait.

Enfin, dans un souci d'information complète des personnes, la Commission a recommandé que la mention d'information relative au droit d'opposition soit accessible en bas de la page consacrée aux « Pages jaunes » sur internet et sur la page écran présentant les photos des habitations. De même, il a été demandé à « Pages Jaunes » d'informer les abonnés de l'existence de ce service dans l'annuaire papier, et d'y rappeler les conditions d'exercice du droit d'opposition.

II. LA POSTE ET LES CHANGEMENTS D'ADRESSES

A. Du fichier des changements d'adresses au fichier national des « nouveaux voisins »

Sur les trois millions de foyers qui déménagent chaque année, deux millions et demi informent La Poste de leur changement d'adresse en souscrivant un contrat dit de réexpédition du courrier, service facultatif et payant permettant de faire procéder au ré-acheminement de son courrier vers sa nouvelle adresse. A cette occasion, La Poste commercialise les nouvelles adresses sauf si les personnes concernées s'y sont opposées. À l'heure actuelle, ce sont 20 % des souscripteurs au contrat de réexpédition qui s'opposent — en cochant la case apposée sur le contrat dit de « réexpédition définitive » — à la cession de leurs nouvelles coordonnées.

Le fichier dit des « changements d'adresse », a été déclaré à la Commission en 1983 avec comme finalité la « réexpédition du courrier ». La commercialisation a été déclarée en 1992 mais à l'époque, seules les sociétés déjà en possession de l'ancienne adresse étaient concernées. Lors de l'examen de ce traitement par la Commission *[cf.* 13e rapport annuel 1992, p. 104), une attention toute particulière avait été portée aux mentions d'information des personnes concernées. La formulation proposée était apparue insuffisante à la Commission qui avait souhaité que soient mentionnées dans le formulaire de réexpédition du courrier et le projet de décision de La Poste les autorités auxquelles La Poste est tenue de communiquer les changements de domicile dont elle a eu connaissance (service des contributions directes et régisseur de la redevance de l'audiovisuel) en vertu de l'article L. 5 du Code des postes et télécommunications.

L'examen du dossier en séance avait également fait apparaître les inquiétudes des commissaires relatives au risque que ce traitement ne soit le prélude à la mise en œuvre d'un fichier central des adresses qui pourrait jouer le rôle d'un fichier dit de population.

Le nouveau traitement sur lequel la Commission s'est prononcée à deux reprises consiste désormais — selon une conception très extensive du voisinage — à permettre à tout organisme, et pas seulement à ceux en possession de l'ancienne adresse des usagers, de disposer des nouvelles adresses.

Lors de la première présentation du dossier, la Commission avait formulé plusieurs réserves ayant pour objet notamment que La Poste s'engage à ne procéder à aucun « enrichissement » de ses fichiers avec des fichiers appartenant à des sociétés tierces, et que la mention d'information sur le bordereau de souscription de changement d'adresse définitif soit rédigée en prévoyant un système de double case à cocher, afin de distinguer l'opposition à la cession de la nouvelle adresse aux organismes qui détenaient l'ancienne adresse de l'opposition à la cession des organismes qui ne la détenaient pas.

La Poste faisant état de difficultés pratiques et financières à mettre en œuvre les recommandations de la CNIL concernant la double case à cocher, un nouvel examen en séance plénière a eu lieu le 11 mars 2003. La délibération n° 03-011 prend ainsi acte de ce que La Poste s'est engagée à ne procéder à aucun « rapprochement » des fichiers de La Poste avec des fichiers appartenant à des sociétés tierces ; que les visas du nouveau projet de décision font désormais référence aux différentes décisions prises précédemment par La Poste dans le cadre de la gestion des contrats de réexpédition du courrier ; que la décision est désormais rédigée conformément à la délibération n° 02-071 du 15 octobre 2002.

La seule modification par rapport à la délibération susvisée concerne la rédaction de la mention d'information sur les contrats de souscription. En effet, la Commission a considéré que la formulation proposée par La Poste était plus explicite s'agissant de la finalité de la cession puisqu'il sera précisé que La Poste souhaite commercialiser et non plus communiquer les données, et plus simple d'utilisation pour les intéressés avec une seule case à cocher. Cette mention sera donc rédigée de la manière suivante :

« La Poste souhaite commercialiser tout ou partie des informations collectées sur le formulaire, aux organismes qui en feraient la demande et qui ne détiennent pas tous votre ancienne adresse (banques, entreprises, commerces, associations, etc.).

« En cas de désaccord, veuillez cocher la case ci-contre : D

« *Quelle que soit votre réponse, votre changement d'adresse sera traité dans les conditions habituelles.*

« Les indications recueillies ci-dessus donnent lieu à l'exercice d'un droit de rectification auprès du bureau de Poste de votre *choix ou auprès de votre centre opérationnel de l'adresse conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

« Dans tous les cas, La Poste est tenue de notifier les changements de domicile au service des contributions directes et au service de la redevance de l'audiovisuel conformément aux dispositions de l'article 92 de la loi n° 85-1407 du 30 décembre 1985 ».

Il est intéressant de noter que le commissaire canadien à la protection de la vie privée, dans son rapport annuel au Parlement 2001-2002, fait état de démarches similaires tendant à instaurer une plus grande transparence dans les échanges auxquels procède la Société canadienne des postes. Saisi d'une plainte relative aux conditions de cession à des fins commerciales des nouvelles adresses des personnes s'inscrivant au service des changements d'adresse pour faire réexpédier leur courrier, le commissaire canadien a fait valoir les mêmes arguments. Même souci qu'apparaisse clairement la vente des nouvelles adresses des abonnés aux entreprises de marketing direct lors de la souscription du contrat de réexpédition. Même importance donnée à la possibilité de s'opposer à une telle cession : la Société canadienne des postes a finalement accepté le principe de la case à cocher figurant sur ce même contrat.

B. Les quiproquos du changement d'adresses

Parfois sans conséquences graves, les « dysfonctionnements » des systèmes informatiques peuvent, dans certains cas, se révéler très préjudiciables pour les personnes concernées.

Ainsi, par exemple, à la suite d'une erreur commise par sa banque, le relevé de compte de M^me^ M. est adressé à son fils, demeurant à une autre adresse.

Interrogée sur ce dysfonctionnement, la banque indique à la Commission qu'elle a réalisé une mise à jour de son fichier de clients par rapprochement avec le fichier national des changements d'adresses de La Poste, à l'aide du traitement « Charade ».

La banque expose que lors de cette opération de recoupement, le rapprochement des prénoms, s'effectuant sur huit caractères, a eu pour conséquence d'opérer une confusion entre le prénom de la cliente, « Marie-Françoise », et celui de son fils, « François ». Cette confusion a été rendue possible par le fait que son fils François était auparavant domicilié à la même adresse que sa mère et qu'il avait fait récemment un changement d'adresse enregistré dans le fichier géré par La Poste.

Cette confusion a entraîné la modification automatique du fichier client de la Caisse d'Épargne, prenant en compte l'information selon laquelle sa cliente aurait déménagé.

La CNIL a saisi La Poste de ces faits, soulignant que l'erreur qui a été à l'origine de l'envoi du relevé de compte de la requérante à son fils était due à un malheureux concours de circonstances mais aussi au mode de recoupement utilisé par le système « Charade » de La Poste. Un contrôle de la civilité qui est enregistrée dans le système « Charade » (« Madame » en lieu et place de « Monsieur ») aurait en effet dû permettre d'éviter une confusion entre la requérante et son fils.

M. J. a lui aussi saisi la CNIL d'une situation comparable, qui a eu pour conséquence l'envoi de ses relevés de compte bancaire à la nouvelle adresse de son épouse, alors qu'il est en instance de divorce.

III. LA MISE EN ŒUVRE ET L'EXPLOITATION DU RECENSEMENT

En 2002, la CNIL a eu à se prononcer à la fois sur le recensement de 1999 et sur celui de 2004-2008.

A. La mise en œuvre du nouveau recensement

La CNIL a été saisie par l'INSEE d'un projet de décret pris en application de l'article 158 de la loi n° 2002-276 du 27 février 2002 relative à la démocratie de proximité qui met en place le nouveau recensement de la population. Cette loi a été

votée, suite à l'avis du Conseil d'État du 2 juillet 1998 selon lequel le législateur devait se prononcer eu égard à l'ampleur de la rénovation souhaitée et aux conséquences que les modalités de détermination de la population légale induisent dans la vie nationale.

On rappellera que, dès 1999, la CNIL a eu à examiner, en raison non seulement des lourdeurs de mise en oeuvre et du coût du recensement classique, mais également des réticences exprimées par la population vis-à-vis du recensement général de 1999, une nouvelle procédure de recensement de la population visant à permettre aux acteurs nationaux et locaux de disposer d'informations régulières et récentes (résultats annuels) pour conduire dans de meilleures conditions leur politique économique et sociale.

1. DE NOUVELLES METHODES : ROTATION ET ÉCHANTILLONS

Les nouvelles méthodes de recensement, telles qu'elles sont définies par l'article 156 de la loi précitée, consistent à opérer par la voie :
— d'un recensement classique (exhaustif) dans les communes de moins de 10 000 habitants mais selon un principe de rotation annuelle (une commune sur cinq étant recensée chaque année) ;
— d'une enquête par sondage dans les communes de 10 000 habitants ou plus, effectuée chaque année auprès de 8 % de la population totale de la commune. Ainsi, au bout de cinq ans, l'ensemble du territoire de ces communes aura été pris en compte et 40 % de la population recensée. Pour mener à bien le recensement dans les dites communes, l'INSEE a créé le répertoire des immeubles localisés (RIL)[1] : le territoire communal est réparti en cinq groupes d'immeubles et, chaque année, une partie des adresses d'un groupe est sélectionnée et les logements situés à ces adresses sont recensés.

Cette méthode de sondage, fondée sur une base exhaustive d'adresses, permettrait de vérifier que l'information nécessaire a bien été collectée, qu'aucune omission n'a été faite, et par extrapolation, de produire des statistiques portant sur toute la population, et non pas seulement sur les personnes directement interrogées.

Quelle que soit la taille des communes, pour apprécier les évolutions intervenues et appliquer celles-ci aux données collectées sur le territoire, l'INSEE est habilité à utiliser des données démographiques non nominatives extraites de fichiers administratifs (notamment les fichiers de l'assurance maladie, les fichiers de la taxe d'habitation...).

Le recensement de la population 2004-2008 concernera la France métropolitaine, les départements d'outre-mer et Saint-Pierre-et-Miquelon. Les enquêtes de recensement auront lieu chaque année de mi-janvier à mi-février (fin février pour les plus grandes communes).

[1] Le RIL a été créé par un arrêté du 19 juillet 2000 pris après avis de la CNIL (délibération n° 039 du 4 juillet 2000), modifié par un arrêté du 8 novembre 2002.

L'article 157 de la loi de février 2002 prévoit qu'en Nouvelle-Calédonie, en Polynésie française, à Mayotte et dans les îles Wallis et Futuna, le recensement de la population sera réalisé tous les cinq ans.

2. LES OBSERVATIONS DE LA CNIL

Les dispositions du projet de décret soumis à la CNIL concernant plus particulièrement l'application de la loi du 6 janvier 1978 figurent d'une part dans le titre III relatif au traitement dénommé « Recensement de la Population », d'autre part, dans le titre I (article 19) qui autorise la collecte et le traitement de données relevant de l'article 31 pour les recensements en Nouvelle-Calédonie et à Mayotte. La CNIL en a délibéré le 19 décembre 2002.

a) Le rôle des communes

Le projet de décret définit le champ de compétence des communes ou des établissements publics de coopération intercommunale (EPCI) et celui de l'INSEE. Les communes ou les EPCI procèdent au recensement des logements, ainsi que des personnes sans abri et des personnes résidant dans des habitations mobiles terrestres présentes sur le territoire de la commune à la date du début de la collecte des données. L'INSEE est chargé de recenser les communautés et les mariniers.

La Commission a pris acte de la possibilité ouverte désormais aux personnes recensées de renvoyer leurs bulletins directement à la direction régionale de l'INSEE dont elles relèvent, et non plus directement aux communes. Elle a estimé qu'il appartenait à l'INSEE de porter à la connaissance de la population cette possibilité de retour direct des questionnaires.

Il est à signaler, en ce qui concerne les données de localisation des immeubles utiles à la réalisation des enquêtes de recensement, que la Commission a admis la pertinence de la connaissance du nom de l'occupant principal pour assurer l'exhaustivité de la collecte. La qualité du recensement repose sur cette exhaustivité et donc, sur celle du recensement des logements à une adresse donnée.

b) Les phases du recensement

Le projet de décret précise également les cinq phases du recensement (la Collecte des données, le contrôle de l'exhaustivité des enquêtes, le contrôle de la cohérence des réponses aux enquêtes, la saisie et l'exploitation des données collectées, la diffusion des informations issues des données collectées), ainsi que les enquêtes de recensement susceptibles d'être mises en œuvre : les enquêtes auprès des personnes vivant dans des logements (à l'exception de celles vivant dans les communautés), les enquêtes auprès des personnes résidant dans les habitations mobiles et celles menées auprès des personnes sans abri. Elles relèvent du champ de compétence des communes ou des EPCI, sous le contrôle de l'INSEE.

S'agissant des enquêtes de recensement, menées conjointement par l'INSEE et les communes ou les EPCI, il est précisé que seules sont visées les deux premières phases, la collecte des données et le contrôle de l'exhaustivité des enquêtes.

Les trois dernières phases, qui seront mises en oeuvre par l'INSEE, feront l'objet d'arrêtés, pris après avis de la CNIL.

La Commission a pris acte de ce que le dispositif de collecte des données auprès des personnes était sensiblement le même que celui de 1999. L'agent recenseur contactera les personnes vivant dans le logement à enquêter, y déposera les bulletins individuels et la feuille de logement, puis viendra récupérer ces documents une fois remplis. Ils seront stockés par la commune ou l'EPCI, puis transmis à l'INSEE dans un délai de dix jours francs après la fin de la collecte.

Il est par ailleurs prévu un droit d'accès et de rectification des personnes aux données les concernant auprès des directions régionales de l'INSEE.

Les informations susceptibles d'être recueillies sont relatives :
— à la localisation des immeubles ;
— aux personnes physiques résidant dans le logement recensé : la date et le lieu de naissance, le sexe, la nationalité, la situation familiale, le niveau et la nature de la formation, les études, les activités professionnelles, le lieu de résidence, le lieu d'étude ou de travail, la résidence antérieure, les moyens de transport, les conditions de logement et l'équipement en véhicules automobiles ;
— aux caractéristiques et aux éléments de confort des logements recensés ;
— aux immeubles bâtis : année de construction et caractéristiques d'équipement.

La Commission a demandé que le décret soit complété pour faire mention, au titre des données collectées, du nom et des prénoms des personnes, étant précisé que ces données ne figurent pas dans le fichier de saisie informatisé.

En cas d'impossibilité de joindre les occupants à une adresse, une fiche d'enquête non aboutie (FENA) sera établie. Les données recueillies sont relatives à la localisation précise et la catégorie du logement, au nom de l'occupant principal, à la raison de l'impossibilité de la collecte, au nombre de personnes supposées y résider.

c) Les traitements de gestion

L'INSEE, les communes ou les EPCI mettront en place des traitements destinés à suivre l'avancement de la collecte. Les communes devront ainsi transmettre, chaque semaine à l'INSEE, des indicateurs sur le nombre de logements recensés depuis le début de la collecte, le nombre de bulletins individuels collectés et le nombre de logements dont le recensement n'a pas été possible.

Ces traitements qui permettront aux communes le calcul de la rémunération des agents recenseurs n'ont pas appelé d'observation particulière de la Commission, les seules informations nominatives recueillies concernant les noms des agents recenseurs.

L'INSEE, les communes ou les EPCI auront aussi la possibilité de mettre en place des enquêtes de contrôle d'exhaustivité.

Alors que le contrôle de l'exhaustivité de la collecte, effectué pour les recensements de 1990 et 1999, consistait à comparer pour une zone considérée, la liste des logements identifiés sur le terrain par les agents recenseurs au nombre de logements résultant de l'exploitation des fichiers de la taxe d'habitation, il s'agit, au cas présent, de procéder à une nouvelle enquête portant sur la localisation précise et la catégorie du logement, sur le nombre de logements à l'adresse et le nombre de personnes par logement.

L'arrêté du 22 mai 1998 relatif au recensement de 1999 autorisait l'INSEE, pour cette finalité, à utiliser les données du fichier de la taxe d'habitation. Pour le nouveau recensement, les modalités de contrôle seraient sensiblement différentes, puisque les communes ou les EPCI pourraient également utiliser pour ce contrôle de l'exhaustivité de la collecte, des informations extraites du fichier de la taxe d'habitation auxquels ils ont déjà accès. Les données collectées, à cette fin, doivent être détruites dans les trente jours francs suivant la fin de la collecte.

Comme la loi de 2002 prévoit que les données de localisation des immeubles sont librement échangées pour la préparation et la réalisation des enquêtes de recensement, mais aussi que ces données sont couvertes par le secret statistique, la CNIL a cru devoir rappeler que le respect du principe de finalité impose que lesdites informations ne soient pas utilisées à d'autres fins. La Commission a donc demandé que le projet de décret soit complété sur ce point.

d) Les données sensibles

Le projet de décret vise à autoriser, en application de l'article 31 de la loi du 6 janvier 1978, à l'occasion des recensements de population :
— en Nouvelle-Calédonie, la collecte et le traitement des données nominatives sus ceptible de faire apparaître l'origine ethnique des personnes ;
— à Mayotte, la collecte et le traitement des données nominatives relatives à la poly gamie et au statut civil des personnes.

Dès 1983 (délibération n° 83-12 du 18 janvier 1983), puis en 1989 (délibération n° 89-02 du 10 janvier 1989) et en 1995 (délibération n° 95-116 du 17 octobre 1995), la Commission a considéré que le recueil de l'appartenance ethnique des personnes, compte tenu des caractéristiques socio-démographiques propres au territoire de la Nouvelle-Calédonie, répondait à un motif d'intérêt public au sens de l'alinéa 3 de l'article 31.

À l'instar des recensements de 1997 et 2002, il est prévu de procéder à Mayotte au recueil de l'information sur la polygamie des personnes et leur statut civil (personnel ou de droit commun). Le recueil de ces données étant susceptible de faire apparaître l'origine ethnique, les opinions religieuses des personnes ainsi que leurs mœurs, la Commission a considéré lors des précédents recensements, compte tenu des spécificités sociales propres à la collectivité départementale de Mayotte, que le recueil de ces informations répondait à un motif d'intérêt public, au sens de l'alinéa 3 de l'article 31 de la loi du 6 janvier 1978 *(cf.* délibération n° 97-028 du 1er avril 1997 et délibération n° 02-012 du 14 mars 2002).

La Commission a donc également émis un avis conforme au projet de décret portant application des dispositions de l'article 31 de la loi du 6 janvier 1978.

B. L'archivage du recensement de 1999

La Commission a été saisie par la direction des Archives de France d'une demande de conseil concernant les modalités d'archivage des fichiers électroniques issus de l'exploitation des données du recensement général de la population (RGP) de 1999.

1. LES CARACTERISTIQUES DES FICHIERS DU RECENSEMENT

Lors du recensement de 1999, l'INSEE a innové en décidant de recourir à la technique de la lecture optique, pour exploiter les bordereaux du recensement.

L'arrêté du ministre de l'Economie, des Finances et de l'Industrie du 29 juillet 1998 pris après avis de la CNIL (délibération n° 98-076 du 7 juillet 1998), qui porte création d'un traitement automatisé par lecture optique des bulletins du RGP, a officialisé la création de trois bases d'images :

— la base image « nom-prénoms-naissance » (nom, prénoms, date et lieu de naissance des personnes recensées) ;

— la base image « adresse du logement » (adresse précise du logement recensé et nom du ménage y résidant à la date du recensement) ;

— la base image « complète non nominative » (toutes les données issues des feuilles de logement et des bulletins individuels à l'exclusion de l'adresse du logement, du nom et des prénoms des personnes).

Ce texte prévoit qu'aucun rapprochement entre les trois bases ne pourra être réalisé. Son article 5 énonce par ailleurs que les seuls destinataires des bases d'images sont l'INSEE et les Archives de France.

2. LA DEMANDE DES ARCHIVES DE FRANCE

La direction des Archives de France, du fait de la numérisation des questionnaires, a ainsi pour la première fois depuis le recensement de 1962, l'opportunité de conserver l'ensemble des documents du recensement de 1999, dernier recensement du millénaire, lesquels lui permettront de disposer d'une vue exhaustive de la population française à la fin du second millénaire.

Il est toutefois apparu que les bases images, constituées par l'INSEE pour ses propres besoins, n'étaient pas, en l'état, utilisables par les Archives de France et nécessitaient en conséquence un nouveau traitement afin de permettre leur exploitation et leur diffusion au public à l'expiration du délai de cent ans fixé par la loi du 3 janvier 1979. En effet, aux termes de l'article 35, « *les recensements et enquêtes statistiques effectués conformément à la loi n° 51-711 du 7 juin 1957 ont le caractère d'archives publiques.* » Son article 7 fixe par ailleurs le délai à l'expiration duquel les données du recensement seront communicables : toute communication est

interdite avant cent ans à compter de la date du recensement ou de l'enquête. Aucune dérogation ne peut être accordée avant l'expiration de ce délai.

En raison de la fragilité des supports et de la rapide obsolescence des matériels et des logiciels, mais également de la fragilité supplémentaire créée par le découpage en trois bases, la direction des Archives de France a insisté sur la relative urgence qu'il y avait à procéder d'ores et déjà à un traitement spécifique des fichiers afin de reconstituer une base unique. À l'appui de sa demande, elle indiquait que toutes les garanties seraient offertes pour assurer la sécurité et la confidentialité des données.

La Commission a donc dû se prononcer sur le point de savoir si la direction des Archives de France pouvait être autorisée, au titre des missions qui lui sont dévolues, à reconstituer une base unique, alors même que l'arrêté précité du 29 juillet 1998, précise expressément qu'aucun rapprochement entre les trois bases ne pourra être effectué.

Lors de sa réunion du 10 décembre 2002, la Commission, tout en prenant en considération l'intérêt historique qui s'attache à la conservation de l'ensemble des données du recensement de 1999 et le caractère non communicable desdits fichiers avant l'expiration d'un délai de cent ans, a estimé que la constitution d'une base unique concernant toutes les personnes recensées méconnaîtrait les garanties de confidentialité et d'anonymat qui ont entouré les opérations du recensement général de la population.

En conséquence, la Commission s'est prononcée en faveur du maintien des trois fichiers sur des supports physiques distincts auxquels serait jointe une documentation technique complète et détaillée sur leurs caractéristiques techniques, qui permettrait, au fil du temps, des migrations vers des supports de stockage adaptés à l'évolution de la technologie.

C. La confection et la diffusion d'indicateurs sur les revenus et impôts des ménages

La demande de statistiques locales sur le montant des revenus et la fiscalité de base des ménages est croissante ; elle émane d'horizons variés : collectivités locales réalisant une étude préalable pour l'implantation d'un équipement public, chercheurs en sociologie, en géographie ou en économie, entreprises procédant à une étude de marché... Jusqu'à présent, seule la direction générale des impôts assurait la diffusion de ces statistiques. Le souhait de l'administration d'élargir la diffusion de ces produits statistiques l'a conduite à faire appel au savoir-faire de l'INSEE, sur le fondement de la loi du 7 juin 1951 sur les statistiques qui autorise la cession à l'Institut national de la statistique des informations nominatives traitées par les administrations *« aux fins exclusives d'établissement de statistiques »*.

Pour répondre à cette demande, l'INSEE a prévu la confection et la diffusion, pour les habitants de zones au moins égales à un quartier IRIS 2000, de statistiques sur le revenu fiscal des ménages, l'impôt sur le revenu et la taxe d'habitation perçue

au titre d'une résidence principale. Bien que s'inspirant des modalités de diffusion des résultats du recensement de la population, le projet s'en distingue sur plusieurs points, notamment sur la priorité donnée à la diffusion d'indicateurs de distribution qui expriment à la fois le niveau des revenus et impôts des ménages et leur répartition au sein d'une population et assurent une meilleure préservation de la confidentialité des situations individuelles.

Saisie de ce projet, la CNIL s'est prononcée favorablement par une délibération du 24 janvier 2002. La Commission a d'abord insisté sur la nécessité d'entourer de mesures de sécurité renforcées la base nationale des informations fiscales sur l'ensemble des ménages, dès lors que celles-ci seront indirectement nominatives du fait de la précision de leur niveau de localisation. Elle a également demandé que les seuils de diffusion applicables à certains produits statistiques soient rehaussés par rapport à ceux retenus pour le recensement, afin de tenir compte de la sensibilité particulière des informations traitées — elles se rapportent à la situation déclarée par les foyers fiscaux — et du risque spécifique de réidentification indirecte des personnes pour des secteurs faiblement peuplés — parfois l'information diffusée ne concerne pas la totalité de la population de la zone mais les seules personnes imposables.

Par exemple, les moyennes de l'impôt sur le revenu et de la taxe d'habitation par ménage, ainsi que les quartiles d'impôt sur le revenu et de taxe d'habitation, ne pourront être diffusés que s'ils se rapportent au moins à un regroupement de trois IRIS 2000 ou à des communes ou groupements de communes de 5 000 habitants. Des fichiers-détail, constitués par ménage, ne pourront être communiqués que pour des zones représentant une population d'au moins 50 000 ménages, soit un minimum de 100 000 habitants. Enfin, les indicateurs additifs ne pourront pas être diffusés pour des zones *ad hoc* définies par les organismes requérants, afin d'éviter tout recoupement des zones géographiques sur lesquelles ils portent.

IV. LE PORTAILWWW.NET-ENTREPRISES.FR

Après avoir clairement fait part de ses orientations sur la question dans son précédent rapport d'activité[1], la CNIL a suivi avec une attention toute particulière les développements de « l'administration électronique » en France au cours de l'année 2002. La Commission a ainsi été amenée à examiner le projet de dématérialisation des déclarations sociales incombant aux entreprises, domaine qu'elle avait déjà eu l'occasion d'aborder dès 1997 à l'occasion du projet de « transferts de données sociales par internet (TDS-net) »[2].

[1] CNIL, 22' rapport d'activité 2001, p. 104 et suivantes disponible sur www.cnil.fr

[2] *Cf.* délibérations du 11 mars 1997 et du 8 décembre 1998. La Commission s'est toutefois prononcée dès 1983 sur les premières procédures dématérialisées de déclarations sociales (TDS normes).

A. La volonté du législateur

Dans le cadre du mouvement de dématérialisation des procédures et des actions de simplification des formalités administratives, la loi de financement de la sécurité sociale pour 2002 a introduit dans le Code de la Sécurité sociale un article L. 133-5 qui permet aujourd'hui aux employeurs et aux professions indépendantes de réaliser leurs déclarations sociales obligatoires par voie électronique et de bénéficier d'un service d'aide à l'élaboration des déclarations sociales et des bulletins de paie baptisés « DUCS-I » (déclaration unifiée de cotisations sociales individualisée)[1].

Le groupement d'intérêt public « modernisation des déclarations sociales » (GIP-MDS) a été choisi par les organismes gestionnaires de régimes de protection sociale pour organiser ces téléservices, sur la base de la gratuité et de l'adhésion volontaire des entreprises, au sein du site www.net-entreprises.fr déjà mis en œuvre par ce groupement.

Pour assurer le service DUCS-I et sa sécurisation, le législateur a prévu que le GIP-MDS est autorisé à collecter et conserver le numéro de Sécurité sociale des personnes concernées, dans des conditions fixées par décret en Conseil d'Etat pris après avis de la CNIL. Celle-ci a donc été consultée sur ce texte.

Parallèlement, la Commission a été saisie par le GIP-MDS de trois projets de téléprocédures concernant la DUCS-I, la déclaration commune de revenus des professions indépendantes (DCR) et la déclaration automatisée de données sociales unifiée (DADS-U).

L'approche de ces différents dossiers par la CNIL constitue une parfaite illustration du fait que, loin de tout dogmatisme sur la question, la Commission accompagne et encourage depuis des années le développement de l'administration électronique, dans le respect des principes de protection des données personnelles.

B. Une utilisation du NIR sécurisée et cantonnée à la sphère sociale

La Commission a ainsi été amenée à se prononcer tout d'abord sur les garanties apportées par le projet de décret pris en application de l'article L. 133-5 du Code de la Sécurité sociale en ce qui concerne l'utilisation du NIR dans le cadre du dispositif net-entreprises[2].

Elle a pu constater que cette utilisation est juridiquement fondée dans la mesure où l'ensemble des émetteurs ou des destinataires de cette information (déclarants d'une part, et organismes sociaux d'autre part) sont légalement ou réglementairement autorisés à traiter cet identifiant pour l'établissement et la prise en compte des déclarations sociales obligatoires des employeurs ou des cotisants.

[1] Loi n° 2001-1246 du 21 décembre 2001, article 73-1.

[2] Délibération n° 02-106 portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article L. 133-5 du Code de la Sécurité sociale concernant l'utilisation du NIR dans le cadre des télédéclarations effectuées sur le portail www.net-entreprises.fr

En revanche, le NIR n'est utilisé ni dans le cadre de l'inscription aux différents téléservices du portail net-entreprises, ni dans le cadre de la procédure d'authentification des utilisateurs de ces téléservices.

Toutefois, dans la mesure où la CNIL a été informée, à l'occasion de l'instruction de ce dossier, de la réalisation d'une étude visant à la mise en oeuvre, dans le cadre du programme net-entreprises, d'un procédé d'authentification des déclarants s'appuyant sur l'émission de certificats électroniques personnels normalisés qui pourrait reposer sur l'utilisation du NIR personnel de l'employeur, la Commission a exprimé une réserve de principe à l'égard d'un tel projet.

En effet, la mise en œuvre de ce projet constituerait un précédent en faveur de l'utilisation généralisée du NIR dans le cadre de dispositifs de certificats électroniques délivrés aux citoyens souhaitant acheter ou vendre sur internet, voter à distance, consulter leur e-dossier, etc., et pourrait avoir pour conséquence la constitution, par les sociétés de certification prestataires, de bases de données contenant les références de plusieurs millions d'employeurs ou de leurs délégataires identifiés par leur numéro de Sécurité sociale... Et c'est très précisément cette banalisation de l'utilisation du NIR, en ce qu'elle porte en elle les germes de l'identification de l'ensemble des Français sur la base d'un identifiant unique dans les fichiers publics ou privés sans lien avec la sphère sociale, que la CNIL s'est toujours employée à dénoncer[1].

Au-delà, la Commission s'est assurée de la mise en œuvre de conditions de traitement sécurisées du NIR — et conséquemment des autres données nécessaires à l'élaboration des déclarations sociales — lors de leur collecte, de leur transmission et de leur conservation. En particulier, ces données doivent faire l'objet d'un chiffrement lors de leur acheminement vers les organismes sociaux.

La Commission a pris acte des engagements du GIP-MDS en ce domaine, et a obtenu d'être rendue destinataire, chaque année, d'un rapport d'évaluation de la sécurité du dispositif.

Dans un souci de cohérence, la CNIL a enfin considéré que les garanties précédemment décrites s'agissant de l'utilisation du NIR dans le cadre du téléservice DUCS-I, devaient également s'appliquer à l'ensemble des téléservices nécessitant une utilisation du NIR des personnes concernées.

C. Sécurisation et transparence autour des téléservices

Désigné par les organismes gestionnaires de régimes de protection sociale pour gérer les téléservices prévus par l'article L. 133-5 du Code de la Sécurité sociale, le GIP-MDS a saisi la Commission des projets « net-DUCS-I », « net-DADS-U » et « net-DCR » [2].

[1] Sur les enjeux liés à la généralisation du NIR, *cf.* 20e rapport d'activité de la CNIL, p. 61 et s., et 22* rapport d'activité, p. 110.

[2] Délibérations n° 02-107, 02-108 et 02-109 relatives à des demandes d'avis présentées par le GIP-MDS pour la mise en œuvre des télédéclarations net-DUCS-I, net-DADS-U et net-DCR sur le portail www.net-entreprises.fr

Le téléservice net-DUCS-I est destiné à simplifier les déclarations des entreprises en regroupant, en une déclaration unique, l'ensemble des obligations déclaratives des employeurs en matière de déclarations de cotisations sociales : établissement de la déclaration unifiée de cotisations sociales (DUCS), acquittement du montant des cotisations par téléréglement, élaboration de déclarations connexes (DADS, attestation employeur...) et, enfin, aide à l'élaboration des bulletins de paie.

La déclaration automatisée de données sociales unifiée « DADS-U » est, quant à elle, le fruit d'une réflexion conduite depuis plusieurs années par la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) et les fédérations de retraite complémentaire AGIRC et ARRCO afin de regrouper en une déclaration unique la déclaration annuelle de données sociales (DADS) mise en œuvre par la CNAVTS pour le compte des partenaires du dispositif « transfert de données sociales (TDS) » et la déclaration annuelle de données sociales des caisses de retraite complémentaire (DADS-CRC) à destination des institutions de retraite complémentaire et des institutions de prévoyance.

Enfin, le téléservice net-DCR permet la numérisation de la déclaration commune des revenus des professions indépendantes existant sur support papier (sans entraîner de modification sur le fond) et la simplification de la procédure déclarative (grâce à un pré-remplissage des déclarations). Les destinataires finaux des informations demeurent les gestionnaires nationaux et locaux de la Caisse nationale d'assurance maladie des professions indépendantes (CANAM), de l'Agence centrale des organismes de Sécurité sociale (ACOSS), de l'ORGANIC et de la Caisse autonome nationale de compensation d'assurance vieillesse des artisans (CANCAVA).

Dans la mesure où les téléservices concourent à la constitution, par le GIP-MDS, de bases de données nominatives relatives aux déclarants et aux salariés des entreprises ayant souhaité adhérer aux dispositifs, la Commission a considéré que la sécurisation des échanges, des sessions de télédéclaration ou de consultation, et du stockage des données constituait un impératif. Elle a par conséquent demandé la mise en oeuvre de mesures de sécurité fortes autour de ces téléservices afin que soit garanti un haut niveau de confidentialité et d'intégrité des données traitées.

Au-delà des mesures initialement envisagées, la CNIL a également demandé le renforcement des sécurités par l'exploitation régulière d'un dispositif de journalisation des connexions et par l'insertion d'une clause de confidentialité dans le contrat liant le GIP-MDS à l'entreprise assurant l'hébergement des serveurs de télédéclaration.

La Commission s'est en outre attachée à rappeler aux entreprises adhérentes leur obligation d'information de leurs salariés sur l'utilisation de ces téléservices.

Enfin, compte tenu du caractère novateur et sensible de tels dispositifs, la Commission a demandé à être rendue destinataire d'un bilan de leur mise en oeuvre à l'issue de la première année d'exploitation.

DEUXIÈME PARTIE

LES DÉLIBÉRATIONS 2002 PAR SECTEUR D'ACTIVITÉ

Banque

Délibération n° 02-110 du 19 décembre 2002 portant avis sur la modification de la loi du 9 juillet 1991 portant réforme des procédures civiles d'exécution visant à permettre aux huissiers d'interroger directement l'administration fiscale détentrice du fichier des comptes bancaires (FICOBA)

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère de la Justice d'un projet de modification de la loi du 9 juillet 1991 portant réforme des procédures civiles d'exécution, et notamment de son article 39, ayant pour objet de permettre aux huissiers de justice de s'adresser directement à la direction générale des impôts pour interroger le fichier des comptes bancaires (FICOBA) ;

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

Vu la convention du 28 janvier 1 9 8 1 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu ensemble la loi n° 78-17 du 6 janvier 1 978 modifiée relative à l'informatique, aux fichiers et aux libertés et le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi du 6 janvier 1978 précitée ;

Vu ensemble la loi n° 91-650 du 9 juillet 1991 portant réforme des procédures civiles d'exécution et le décret du 31 juillet 1992 instituant de nouvelles règles relatives aux procédures civiles d'exécution pour l'application de la loi n° 91 -650 du 9 juillet 1 991 portant réforme des procédures civiles d'exécution ;

Vu l'arrêté du 14 juin 1982 modifié fixant les modalités d'un système automatisé de gestion du fichier des comptes bancaires ;

Vu la délibération n° 88-072 du 28 juin 1988 portant avis sur un projet de loi de réforme des procédures d'exécution en matière mobilière ;

Après avoir entendu Monsieur Philippe Nogrix, commissaire, en son rapport et Madame Catherine Pozzo di Borgo, commissaire du gouvernement adjoint, en ses observations ;

Formule les observations suivantes :

La direction des affaires civiles et du sceau du ministère de la Justice a saisi pour avis la Commission nationale de l'informatiaue d'un projet de modification de la loi du 9 juillet 1991 portant réforme des procédures civiles d'exécution, et notamment de son article 39, ayant pour objet de permettre aux huissiers de justice de s'adresser directement à la direction générale des impôts pour interroger le fichier des comptes bancaires (FICOBA).

L'article 39 de cette loi ne permet en effet l'accès des huissiers de justice à certaines informations concernant le débiteur (références bancaires, domicile et adresse de l'employeur) que par l'intermédiaire du procureur de la République.

La modification envisagée permettrait aux huissiers de s'adresser directement à l'administration fiscale détentrice du fichier des comptes bancaires (FICOBA) pour obtenir l'adresse des organismes auprès desquels un compte est ouvert au nom

du débiteur. En revanche l'adresse personnelle du débiteur et de celle de son employeur ne pourraient, comme dans le texte en vigueur, être recherchées que sur demande préalable au procureur de la République.

Selon les indications fournies par le ministère de la Justice, qui a réalisé un bilan de cette procédure de recherche d'informations, cette modification trouve sa justification dans la trop grande lenteur et la faible efficacité de cette procédure.

La Commission rappelle qu'elle avait, lors de son avis rendu le 28 juin 1988 sur le projet de loi qui instituait la procédure dont la modification est aujourd'hui souhaitée, considéré que l'intervention systématique du procureur de la République constituait une garantie importante de nature à limiter la communication de ces informations aux seuls cas où elle serait nécessaire.

Elle estime dès lors que la modification souhaitée ne peut être envisagée que si elle est accompagnée de mesures assurant une protection équivalente et réaffirme son souhait de voir instituer un contrôle rigoureux de ses modalités pratiques de mise en œuvre et de fonctionnement, tout particulièrement lors de la refonte en cours du fichier des comptes bancaires.

Une attention particulière devra notamment être apportée à la vérification de la qualité de l'auteur de la requête, de la validité du titre exécutoire dont il est porteur, de la présence d'un relevé certifié sincère de recherches infructueuses, ainsi qu'à celle de la conformité de la demande aux conditions légales de transmission des renseignements.

La Commission considère, à cet égard, que la centralisation des demandes des huissiers et leur traitement par le service central du fichier FICOBA constitueraient des garanties supplémentaires.

La Commission prend également acte qu'aux termes de l'article 41 de la loi du 9 juillet 1991 les renseignements obtenus ne peuvent être utilisés que dans la seule mesure nécessaire à l'exécution du ou des titres pour lesquels ils ont été demandés et qu'ils ne peuvent, en aucun cas, être communiqués à des tiers ni faire l'objet d'un fichier d'informations nominatives.

Au bénéfice des observations qui précèdent, la Commission émet un avis favorable à la modification de la loi du 9 juillet 1991 portant réforme des procédures civiles d'exécution et des textes modifiés en conséquence.

Demande à être consultée sur les modifications réglementaires qui devront en conséquence être apportées au décret du 31 juillet 1992 instituant de nouvelles règles relatives aux procédures civiles d'exécution pour l'application de la loi n° 91-650 du 9 juillet 1991 portant réforme des procédures civiles d'exécution, et notamment son article 54, ainsi qu'à l'arrêté du 14 juin 1982 portant création du fichier des comptes bancaires mis en œuvre par l'administration fiscale.

Biométrie

Délibération n° 02-033 du 23 avril 2002 relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le maire de Goussainville d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité la gestion des pointages du personnel par empreintes digitales (demande d'avis n° 798267) ;

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

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

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

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

Formule les observations suivantes :

La municipalité souhaite procéder à l'installation de deux appareils de reconnaissance biométrique respectivement au rez-de-chaussée et au premier étage de l'hôtel de ville afin de remplacer son système actuel de gestion des pointages par badges magnétiques par un dispositif de reconnaissance d'empreintes digitales. Le traitement biométrique concernerait une centaine d'agents environ.

La municipalité fait valoir que l'utilisation d'un procédé biométrique serait nécessaire du fait du nombre croissant d'oublis, de perte ou de prêt de badge, et que le système ne s'appliquerait qu'au seul personnel de la mairie.

Les gabarits d'empreintes digitales devraient être centralisés dans une base de données située sur le serveur de la salle informatique ; en pratique, chaque agent devrait présenter son pouce droit au lecteur d'empreintes digitales afin que les gestionnaires du personnel et le service informatique puissent calculer son temps de présence au travail.

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

constitution d'une base de données d'empreintes digitales est-elle susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création.

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

Dans le cas d'espèce, l'objectif d'une meilleure gestion des horaires, s'il est légitime, ne paraît pas de nature à justifier l'enregistrement dans une base de données des empreintes digitales des personnels d'une mairie. Aussi le traitement pris dans son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi.

Émet un avis défavorable au projet d'arrêté présenté par la mairie de Goussainville en application de l'article 15 de la loi du 6 janvier 1978 relatif à la mise en oeuvre d'un traitement automatisé d'informations nominatives ayant pour finalité la gestion des pointages du personnel par empreintes digitales.

Délibération n° 02-034 du 23 avril 2002 portant avis sur un projet de décision du directeur général de l'établissement public aéroports de Paris relative à une expérimentation de trois dispositifs biométriques de contrôle des accès aux zones réservées de sûreté des aéroports d'Orly et de Roissy

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet de décision du directeur général des aéroports de Paris concernant la mise en œuvre à titre expérimental de différents systèmes d'identification biométrique se fondant sur la reconnaissance l'un de l'empreinte digitale, l'autre de l'iris et le troisième de la forme de la main des personnes travaillant dans certaines parties à accès réservé des aéroports d'Orly et de Roissy dénommées « zones réservées de sûreté » (demande d'avis n° 799468) ;

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

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

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

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

Formule les observations suivantes :

Les expérimentations de contrôle d'accès par reconnaissance biométrique seraient mises en oeuvre auprès des seuls personnels volontaires d'aéroports de Paris, des services publics et des entreprises exerçant une activité en zone réservée de sûreté des aéroports d'Orly et de Roissy. Chacune d'entre elles serait limitée à six mois.

Les informations collectées auprès des personnes volontaires pour l'expérimentation seraient limitées à l'identité de ces personnes, à leur numéro de titre de circulation en zone réservée et, selon le cas, au gabarit biométrique de leur empreinte digitale, de leur iris ou du contour de leur main.

La conservation des informations nominatives collectées dans le cadre de chacun des traitements biométriques serait limitée à six mois à compter de la mise en oeuvre effective dudit traitement.

Les destinataires des données enregistrées seraient, à raison de leurs attributions respectives, les membres du département études et sûreté d'aéroports de Paris relevant de l'équipe de projet responsable de la mise en œuvre des traitements biométriques, les agents chargés de l'enrôlement, les agents de sûreté opérant sur les lieux de l'expérimentation ainsi que les préposés des fournisseurs des équipements biométriques pour le support technique (formation, maintenance).

Le comité d'entreprise serait saisi de ces expérimentations. Les personnels concernés seraient informés par une communication individuelle de l'objet et des modalités de l'expérimentation, et en particulier du caractère facultatif de cette expérimentation ainsi que de l'existence d'un droit d'accès et de rectification au bénéfice des personnes identifiées.

Les aéroports de Paris se sont également engagés à informer toutes les entreprises et services publics concernés.

Dans le cas d'espèce, le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données sont adaptés et proportionnés à la finalité assignée au dispositif.

En effet, plusieurs éléments biométriques seraient successivement expérimentés, seuls les personnels volontaires seraient soumis à ce dispositif de contrôle d'accès par reconnaissance biométrique et, en tout état de cause, les impératifs de sécurité liés à ces zones sensibles justifient le recours à la constitution de bases de données biométriques à de telles fins.

Émet un avis favorable au projet de décision du directeur général d'aéroports de Paris présenté en application de l'article 15 de la loi du 6 janvier 1978.

Demande à être rendue destinataire, à l'issue de la phase expérimentale, d'un bilan de la mise en œuvre des différents systèmes biométriques.

Délibération n° 02-045 du 18 juin 2002 portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis d'un projet de décision du directeur de l'URSSAF de la Corse relative à un traitement automatisé d'informations nominatives reposant sur la reconnaissance de l'empreinte digitale ayant pour objet de contrôler les accès des agents aux bâtiments de l'URSSAF situés à Ajaccio et Bastia (demande d'avis n° 797265) ;

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

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

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

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

Formule les observations suivantes :

Le projet de l'URSSAF de la Corse a pour finalité de renforcer la sécurité des accès à ses locaux en s'assurant de l'identification et de l'authentification de ses agents par la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale des personnels de l'URSSAF.

Les agents seraient appelés à poser leur doigt aux fins de comparaison avec les gabarits d'empreintes digitales de l'ensemble du personnel, conservés au niveau des lecteurs biométriques.

Le directeur de l'URSSAF fait valoir qu'un renforcement de la sécurité est rendu nécessaire par la situation locale spécifique qui a notamment été marquée par des occupations des locaux et des attentats à la bombe ayant provoqué, en 1996 et en 1999, la destruction partielle des deux sites.

La Commission a déjà exprimé dans divers avis qu'une base de données comportant des éléments biométriques laissant des traces, telles que l'ADN ou l'empreinte digitale, présentait, quelle que soit la légitimité du projet poursuivi par le responsable du traitement, le risque d'être utilisée à des fins autres que celles pour lesquelles elle a été constituée. Ainsi, les technologies de reconnaissance biométrique ne reposant pas sur le stockage des gabarits dans une base de données, ou, lorsqu'une base de données est nécessaire, le recours à un élément biométrique ne laissant pas de traces devraient être, de manière générale, préférés à la prolifération de fichiers de gabarits d'empreintes digitales.

Procédant à un examen particulier de chacun des traitements automatisés d'informations nominatives dont elle est saisie en application de l'article 15 de la loi du 6 janvier 1978, la Commission a toutefois estimé parfaitement justifié le recours à des dispositifs de reconnaissance biométrique reposant sur la constitution d'une base de données d'empreintes digitales à des fins de contrôle d'accès lorsque des impéra-

tifs particuliers de sécurité pouvaient l'exiger dans des cas limités ne laissant pas augurer de leur éventuelle généralisation à de telles fins.

Compte tenu du contexte particulier de la demande d'avis qui lui est soumise, la Commission a conduit le 21 mai 2002 une mission d'information auprès de l'URSSAF de la Corse afin de déterminer si le dispositif projeté était de nature à atteindre l'objectif que l'URSSAF s'assigne, dans des conditions garantissant tout à la fois son efficacité et son caractère proportionné.

L'impératif de sécurité n'est pas contesté, comme les graves événements passés en attestent l'évidence.

La Commission a cependant constaté que, s'agissant de l'antenne de Bastia, la disposition des locaux de l'URSSAF situés sur un étage d'immeuble auquel on ne peut accéder qu'après avoir franchi un hall d'accueil contrôlé par un agent et le faible nombre d'agents concernés (sept personnes) ne paraissaient pas justifier, dans des conditions garantissant la proportionnalité entre l'objectif poursuivi et les moyens mis en œuvre, un dispositif de reconnaissance des empreintes digitales des personnels alors que, de surcroît, les autres personnes travaillant ou habitant cet immeuble n'y seraient pas soumises.

S'agissant de l'antenne d'Ajaccio, le dispositif de reconnaissance de l'empreinte digitale destiné à authentifier les personnels ne serait mis en œuvre qu'à l'entrée des locaux et ne pourrait pas l'être à l'entrée du parc de stationnement, les variations locales de température et d'hygrométrie altérant considérablement les performances du système, selon le prestataire lui-même. Dès lors, la Commission ne peut que constater que ce nouveau dispositif de sécurité serait, en tant que tel, impropre à prévenir le renouvellement d'événements de la nature de ceux dont l'URSSAF d'Ajaccio a déjà été la victime.

Ces éléments de fait paraissent suffisamment déterminants, eu égard à la technologie biométrique envisagée, pour que la Commission ne soit pas en mesure de se prononcer par un avis favorable à la mise en œuvre du dispositif qui repose sur la constitution de bases de données d'empreintes digitales des personnels de l'URSSAF alors que, de surcroît, le recours à un système d'authentification par empreinte digitale dont le gabarit serait inclus dans la carte à puce sans être stocké par ailleurs au niveau du lecteur permettrait de garantir que seules des personnes habilitées et reconnues auraient accès aux locaux de l'URSSAF.

Compte tenu de ces observations, la Commission **émet un avis défavorable** au projet de décision du directeur de l'URSSAF de la Corse présenté en application de l'article 15 de la loi du 6 janvier 1978.

Délibération n° 02-070 du 15 octobre 2002 portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Joliot Curie de Carqueiranne, destiné à contrôler l'accès au restaurant scolaire par la reconnaissance de la géométrie de la main

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le principal du collège Joliot Curie de Carqueiranne, en application de l'article 15 de la loi du 6 janvier 1978, d'un projet de décision portant création d'un traitement de gestion de l'accès au restaurant scolaire ;

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

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

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

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

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

Formule les observations suivantes :

Le collège Joliot Curie de Carqueiranne envisage de créer un traitement de gestion des accès au restaurant scolaire des élèves et des personnels, recourant à un dispositif de reconnaissance du contour de la main.

Le système envisagé repose sur la mise en œuvre d'un fichier de gestion comportant l'identité des élèves, leur classe, leur numéro d'ordre dans l'établissement, les coordonnées du responsable légal, un code d'accès personnel ainsi que les données utiles à l'accès au restaurant. Pour les membres du personnel, sont enregistrés l'identité, le code d'accès, l'agenda et le tarif.

Le dispositif de contrôle d'accès est composé d'une borne d'accès, située à l'entrée du restaurant, reliée à un lecteur biométrique, lequel contient une base de données comportant les gabarits biométriques et les codes d'accès. Pour enregistrer l'image de la main d'une personne dans le dispositif, trois mesures sont effectuées de façon à obtenir les dimensions caractéristiques de la main. Cet enregistrement est effectué au début de l'année scolaire.

Lors de chaque passage, la reconnaissance de la main se fait, après avoir saisi sur le clavier du lecteur biométrique, le code d'accès (numéro de référence personnel), en plaçant la main sur un appareil de capture de l'image géométrique de la main. Si la comparaison entre l'image et le gabarit stocké est positive, le lecteur biométrique transmet le code d'accès à la borne qui, pilote le tourniquet d'accès, enregistre la présence et adresse, par le réseau informatique au fichier de gestion la liste des passages (code d'accès, indication de passage).

Les données sont conservées pendant la durée de l'année scolaire ; lorsqu'une personne quitte l'établissement en cours d'année, les données biométriques sont effacées dans la semaine suivant son départ.

Dès lors, tant les informations que leur durée de conservation sont pertinentes et non excessives au regard de la finalité du traitement.

Le recours à la technique de reconnaissance du contour de la main permet de s'assurer que les données nécessaires au contrôle de l'accès ne sont ni perdues, ni échangées et que seules les personnes habilitées peuvent accéder au service. Le contour de la main, à la différence des empreintes digitales, ne laisse pas de trace et limite ainsi les risques d'utilisation des données à des fins étrangères à la finalité poursuivie par le traitement.

Le traitement apparaît dès lors adapté aux objectifs et aux finalités poursuivis par l'administration du collège.

Prend acte de ce que les personnes concernées qui ne sont pas désireuses d'utiliser la technologie biométrique seront dotées d'une carte à code barre pour accéder au restaurant scolaire.

Émet un avis favorable au projet de décision qui lui est soumis.

Demande qu'un rapport d'exécution lui soit transmis dans les six mois suivant la mise en œuvre de l'expérimentation.

Cybervote

Délibération n° 02-015 du 14 mars 2002 portant avis sur un projet d'arrêté présenté par la mairie de Mérignac concernant l'expérimentation d'un dispositif de vote électronique reposant sur l'utilisation de cartes à microprocesseur comportant les empreintes digitales des électeurs

La Commission nationale de l'informatique et des libertés ;

Saisie par la mairie de Mérignac d'un projet d'arrêté relatif à la mise en oeuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une expérimentation d'un dispositif de vote électronique reposant sur le volontariat des intéressés munis de cartes à microprocesseur comportant leurs empreintes digitales ;

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

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

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

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

Formule les observations suivantes :

La mairie de Mérignac souhaite, à l'occasion des prochaines élections présidentielles et législatives, expérimenter, dans un bureau de vote, un dispositif de vote électronique qui reposerait sur l'utilisation de cartes à microprocesseur comportant les empreintes digitales des électeurs. Ce dispositif serait proposé aux électeurs se portant volontaires pour l'expérimenter lesquels voteraient parallèlement de façon traditionnelle.

Cette application s'inscrit dans le cadre d'un projet européen de vote électronique, dénommé « E-Poll » *(Electronic Polling System for Remote Voting Opérations)* financé par la Commission européenne au titre du programme de recherche européen « Information Society Technology ».

Le projet prévoit que les électeurs volontaires seront dotés de cartes à microprocesseur nominatives comportant leurs empreintes digitales. Ils s'authentifieront en introduisant leur carte à puce dans un lecteur et en apposant leur index sur un capteur relié à un ordinateur. Une fois la vérification d'identité opérée par la confrontation des empreintes, l'ordinateur, relié par réseau au serveur conservant la liste électorale constituée pour l'expérimentation vérifiera si l'électeur figure bien sur la liste électorale ; dans l'affirmative, l'électeur considéré obtiendra alors un certificat de vote qui sera enregistré dans la carte dont il est porteur. Une fois dans l'isoloir, l'électeur insérera sa carte dans un deuxième ordinateur muni d'un écran tactile où apparaissent les noms des candidats, exprimera son vote en appuyant sur le nom choisi puis validera son vote en appuyant son index sur un scanner intégré à l'ordinateur et connecté au serveur gérant la liste nominative servant à l'émargement. Le vote sera alors transmis par réseau sous forme chiffrée à un serveur centralisant les votes qui seraient

comptabilisés par ordinateur en temps réel, étant observé que le décompte ne serait accessible qu'à la clôture du scrutin.

Sur le recours à un dispositif de vote électronique

La Commission rappelle que le secret du suffrage, reconnu à l'article 3 de la Constitution, constitue un des principes fondamentaux de notre démocratie et que seuls, le secret du vote, la sincérité des opérations électorales, la surveillance effective du scrutin et le contrôle *a posteriori* par le juge de l'élection peuvent garantir le principe de la liberté du scrutin.

La CNIL croit dès lors devoir souligner que le recours à l'outil informatique et le cas échéant à des prestataires privés, pour assurer la gestion et le contrôle d'opérations électorales, jusqu'alors assurées et surveillées physiquement et directement par des représentants du corps électoral, sans que l'électeur ait réellement les moyens de vérifier leur régularité, compte tenu de la complexité des procédés techniques mis en oeuvre ne peut qu'appeler une réserve de principe. L'extension éventuelle de ce type de dispositif nécessiterait en tout état de cause, un débat public et une intervention législative, le recours à un dispositif de vote électronique, lors d'élections politiques, étant, en l'état des dispositions en vigueur du Code électoral, dépourvu de base légale.

La Commission prend acte cependant que le dispositif de vote électronique proposé par la mairie de Mérignac n'est pas appelé à se substituer aux procédures de vote traditionnelles, qui seules font foi, et a pour seul objet de tester sa faisabilité technique.

Dans le cadre ainsi défini, il convient d'apprécier si les dispositifs techniques prévus pour assurer le secret du vote et garantir la sincérité du scrutin sont propres à donner des indications utiles sur la faisabilité technique du système.

Sur le déroulement de l'expérimentation

1) La Commission prend note que le fichier nominatif des électeurs servant à l'émargement serait conservé sur un serveur distinct de celui servant à la comptabilisation des votes, aucune liaison n'existant entre les deux machines.

2) La Commission relève également que le vote exprimé ne sera transmis que sous forme chiffrée, sans aucune indication de l'identité de l'électeur et ne pourra être décrypté qu'à l'issue du scrutin, selon des procédures placées sous le contrôle du Président du bureau de vote et de ses assesseurs, détenteurs à cet effet de clés de déchiffrement qui ne peuvent réaliser cette opération que si elles sont utilisées simul tanément.

3) Des dispositifs dits de *firewall* permettront de protéger le système contre toute intrusion informatique extérieure.

4) La Commission estime cependant que nonobstant les dispositions techni ques prévues, il importe que toutes mesures soient prises afin de permettre aux candi dats et aux représentants du corps électoral d'assurer une surveillance effective de l'ensemble des opérations électorales *et en* particulier, de la préparation du scrutin, de l'émargement et du dépouillement. À cet effet, les mesures de sécurité et la pré sente délibération de la CNIL devront être tenues à disposition des électeurs.

5) Par ailleurs, pour ce qui concerne le scrutin présidentiel, la Commission estime que le délégué du Conseil constitutionnel territorialement compétent, désigné pour surveiller les opérations électorales, en vertu de l'article 27 du décret du 8 mars 2001 portant application de la loi du 6 novembre 1962 relative à l'élection du Prési dent de la République au suffrage universel, doit être informé de cette expérimenta-

tion afin qu'il puisse s'assurer du déroulement indépendant des deux opérations organisées le même jour.

6) Un rapport sur le déroulement de l'expérimentation devra être adressé à la CNIL.

Sur le recours aux empreintes digitales

L'enregistrement, sur des cartes à microprocesseur, des empreintes digitales des électeurs a pour objet de s'assurer de leur identité et de l'unicité de leur vote.

La Commission rappelle que le recours aux techniques biométriques ne peut être justifié que dans certaines circonstances où l'exigence de sécurité et d'identification des personnes s'impose tout particulièrement.

Elle prend acte qu'en l'espèce le relevé des empreintes digitales de chaque électeur ne sera enregistré que dans une carte à microprocesseur dont l'électeur sera seul détenteur et qu'aucun fichier d'empreintes digitales ne sera constitué.

Elle estime en conséquence que le recours aux empreintes digitales, dans ces conditions, peut être admis, prenant acte, en tout état de cause, que le dispositif n'est mis en œuvre qu'à titre expérimental et n'a pas vocation à se substituer aux opérations traditionnelles de vote.

Émet, au bénéfice de ces observations, un avis favorable au projet d'arrêté présenté par la mairie de Mérignac relatif à la mise en oeuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une expérimentation d'un dispositif de vote électronique reposant sur le volontariat des intéressés munis de cartes à microprocesseur comportant leurs empreintes digitales, sous réserve que :

— l'article premier soit complété pour faire mention de l'utilisation de cartes à micro processeur comportant les empreintes digitales des électeurs ;

— que l'article 2 précise que les empreintes digitales ne seront enregistrées que sur les cartes et ne donneront lieu à aucune constitution de fichier nominatif ;

— que l'article 3 indique que seuls les personnels habilités de la mairie, de la Préfec ture et des prestataires de service pourront accéder, en tant que de besoin, aux infor mations nominatives nécessaires à l'établissement de la liste électorale ;

— que deux articles supplémentaires soient insérés, l'un indiquant qu'il convient, qu'à l'occasion du scrutin présidentiel, le délégué du Conseil constitutionnel territorialement compétent soit prévenu de cette expérimentation afin qu'il puisse s'assurer du déroulement indépendant des deux opérations organisées le même jour, l'autre précisant qu'un rapport sur le déroulement du scrutin devra être adressé à la CNIL et que les mesures de sécurité prises et la présente délibération de la CNIL devront être tenues à disposition des électeurs.

Délibération n° 02-022 du 2 avril 2002 relative à la demande d'avis présentée par la mairie de Vandosuvre-lès-Nancy concernant l'expérimentation d'un dispositif de vote électronique par internet à l'occasion de l'élection présidentielle

La Commission nationale de l'informatique et des libertés ;

Saisie par la mairie de Vandœuvre-lès-Nancy d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une expérimentation d'un dispositif de vote électronique par internet ;

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

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

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

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

Formule les observations suivantes :

La mairie de Vandœuvre-lès-Nancy souhaite, à l'occasion de la prochaine élection présidentielle, expérimenter un dispositif de vote électronique par internet. Ce dispositif serait proposé à tous les électeurs se portant volontaires pour l'expérimenter, lesquels voteraient parallèlement de façon traditionnelle.

La ville de Vandœuvre-lès-Nancy a passé, pour cette opération, un contrat avec la société américaine élection, corn.

Le projet reposerait sur le dispositif suivant : tous les électeurs de la commune recevraient un code confidentiel (code PIN) et un mot de passe attribués, de manière aléatoire, par la société élection, corn ; le vote pourrait avoir lieu, au choix de l'électeur, soit depuis un domicile connecté à internet, soit dans l'un des lieux publics aménagé à cet effet ; la saisie par chacun des électeurs de son code confidentiel associé au mot de passe permettrait la tenue de la liste d'émargement ; le vote serait transmis sous forme cryptée et stocké dans un serveur faisant fonction d'urne électronique, le décompte n'étant accessible qu'à la clôture du scrutin ; les opérations de vote commenceraient la veille du jour officiel du vote (le samedi) et s'achèveraient en même temps que ce dernier, et ce pour les deux tours de l'élection présidentielle.

Il est précisé dans le dossier de demande d'avis que les présidents de bureaux de vote et les scrutateurs pourraient contrôler le bon déroulement des opérations de façon virtuelle, depuis un ordinateur, au moyen d'un code secret en interrogeant à tout moment un compteur donnant avec précision le nombre de votants.

Si des expérimentations de vote électronique peuvent être menées, dès lors qu'elles ne sont pas appelées à se substituer aux procédures de vote traditionnelles qui seules font foi, dans le but de tester la faisabilité d'un système technique, elles ne sauraient être utilement envisagées, au regard des valeurs énumérées par l'article premier de la loi du 6 janvier 1978 *(« l'informatique 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 ») que si les modalités de leur mise en œuvre ne sont pas de nature à porter une atteinte caractérisée aux principes fondamentaux qui doivent commander les opérations électorales.

À cet égard, la garantie du secret du suffrage constitue un principe fondamental que seuls le caractère personnel et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du scrutin et le contrôle *a posteriori* par le juge de l'élection peuvent assurer.

La Commission a ainsi émis un avis favorable à une expérimentation de vote électronique par carte à puce devant être menée à l'occasion des élections présidentielles et législatives de 2002, dans la mesure où les conditions de sa mise en œuvre sont apparues de nature à assurer l'authentification de l'électeur (par la convocation des électeurs volontaires et l'enregistrement de leur empreinte digitale dans une carte à puce privative qui leur était personnellement attribuée), le caractère personnel du vote (qui s'opérait par écran tactile situé dans un isoloir), ainsi que la possibilité d'un éventuel contrôle des serveurs situés sur le territoire national à des fins d'expertise.

De telles garanties minimales ne sont pas réunies dans le cadre de l'expérience projetée.

En effet, en prévoyant une possibilité de vote à domicile par internet, le dispositif prévu est susceptible de porter atteinte au secret et à la sincérité du vote en ne lui conférant pas le caractère personnel qu'il doit revêtir et en ne garantissant pas qu'il soit dégagé de toute influence ou pression.

En tout état de cause, et au regard des seules dispositions de la loi du 6 janvier 1978, le dispositif projeté ne garantit pas l'authentification et l'identification certaine de l'électeur, l'envoi d'un code d'accès et d'un mot de passe par simple courrier adressé à un domicile où peuvent résider plusieurs électeurs n'excluant pas qu'un même électeur puisse voter plusieurs fois en utilisant le code d'accès et le mot de passe des autres personnes du foyer.

En outre, la procédure de vote envisagée conduirait à ce que l'organisation matérielle du vote dépende de dispositifs techniques situés à New York (transfert de la liste électorale, identification des électeurs ayant voté, établissement de la liste d'émargement, « dépouillement » par exploitation informatique des résultats), échappant ainsi à tout contrôle effectif des autorités nationales compétentes alors que de, surcroît, le dispositif retenu en ce qu'il ne prévoit pas le chiffrement du code d'accès, du mot de passe et de l'expression de son vote par le poste de l'électeur-internaute, ne permet pas de garantir l'anonymat du vote d'un bout à l'autre de l'opération technique ; en effet, si la transmission des informations recourt à un chiffrement SSL, les informations en cause qui associent expression du vote et identification de l'électeur se trouvent « à découvert » une fois transmises et avant d'être enregistrées sous forme cryptée sur le serveur d'exploitation des résultats.

Par ces motifs, émet un avis défavorable au projet d'arrêté présenté par la mairie de Vandœuvre-lès-Nancy.

Délibération n° 02-090 du 28 novembre 2002 relative à la demande d'avis présentée par la mairie d'Issy-les-Moulineaux concernant l'expérimentation d'un dispositif de vote électronique par internet lors des élections des conseils de quartier

La Commission nationale de l'informatique et des libertés ;

Saisie par la mairie d'Issy-les-Moulineaux d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une expérimentation d'un dispositif de vote électronique par internet ;

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

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

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

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

Formule les observations suivantes :

La mairie d'Issy-les-Moulineaux souhaite expérimenter un dispositif de vote électronique par internet qui permettrait aux habitants de la commune s'étant préalablement inscrits de participer à la désignation des membres de conseils de quartier.

Cette application est conduite, sur le plan technique par le consortium « cybervote » dirigé par la société EADS et s'inscrit dans le cadre d'un programme de recherche et de développement financé notamment par la Commission européenne.

Le projet reposerait sur le dispositif suivant :

Les habitants volontaires pour participer à cette expérimentation recevraient par voie postale en recommandé ou par remise en main propre un identifiant et un code confidentiel leur permettant de voter par internet depuis leur domicile ou dans un lieu public équipé d'un terminal relié à internet. Ces personnes entreraient leur identifiant puis leur code confidentiel et adopteraient un mot de passe. Elles choisiraient ensuite le nom d'un candidat, sur l'écran. La validation déclencherait la transmission du « bulletin de vote virtuel » vers le serveur, lequel vérifierait que la personne n'a pas déjà voté et permettrait d'enregistrer le code et l'identifiant de l'électeur en clair ainsi que son vote crypté. Le dépouillement s'effectuerait par l'introduction dans le système d'au moins quatre parties d'une clé privée partagée entre huit scrutateurs. Les données seraient ensuite conservées sur un serveur pendant quinze jours (délai de recours) avant leur effacement.

La Commission observe qu'en vertu de l'article 1 de la loi du 27 février 2002 relative à la démocratie de proximité, il appartient au conseil municipal de décider librement de la composition et des modalités de fonctionnement des conseils de quartier, en particulier des conditions de désignation des membres de ces instances.

Sur le fondement de cette disposition, la mairie d'Issy-les-Moulineaux a décidé que quatre membres de chacun des conseils de quartier seraient élus par les habi-

tants parmi les volontaires, après un appel à candidature, en recourant à un dispositif de vote par internet.

La Commission estime qu'en l'absence d'un cadre juridique fixant les conditions à respecter notamment en ce qui concerne l'anonymat du vote, le recours à ce mode de consultation des habitants peut être admis compte tenu de son caractère expérimental et limité.

Par ces motifs, émet un avis favorable au projet d'arrêté présenté par la mairie d'Issy-les-Moulineaux.

Délibération n° 02-091 du 28 novembre 2002 relative à la demande d'avis présentée par la mairie d'Issy-les-Moulineaux concernant l'expérimentation d'un dispositif de vote électronique par internet lors des élections prud'homales

La Commission nationale de l'informatique et des libertés ;

Saisie par la mairie d'Issy-les-Moulineaux d'un projet d'arrêté relatif à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité une expérimentation d'un dispositif de vote électronique par internet ;

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

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

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

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

Formule les observations suivantes :

La mairie d'Issy-les-Moulineaux souhaite, à l'occasion des élections prud'homales qui se dérouleront le 11 décembre 2002, expérimenter un dispositif de vote électronique par internet. Ce dispositif serait proposé aux électeurs volontaires du collège employeur, lesquels voteraient parallèlement de façon traditionnelle.

Cette application est conduite, sur le plan technique par le consortium « cybervote » dirigé par la société EADS et s'inscrit dans le cadre d'un programme de recherche et de développement financé notamment par la Commission européenne.

Le projet reposerait sur le dispositif suivant :

Les électeurs volontaires pour participer à cette expérimentation recevraient par remise en main propre un identifiant et un code confidentiel leur permettant de voter par internet depuis leur lieu de travail ou dans un lieu public équipé d'un terminal relié à internet. L'électeur entrerait son identifiant puis son code confidentiel et choisirait un mot de passe. Il choisirait ensuite le nom d'une liste, sur l'écran. La validation déclencherait la transmission du « bulletin de vote virtuel » vers le serveur, lequel vérifierait que l'électeur n'a pas déjà voté et permettrait d'enregistrer dans l'urne virtuelle le code et l'identifiant de l'électeur en clair ainsi que son vote crypté. Le dépouillement s'effectuerait par l'introduction dans le système d'au moins quatre parties d'une clé privée partagée entre huit scrutateurs. Les données seraient ensuite conservées sur un serveur pendant quinze jours (délai de recours) avant leur effacement.

Si des expérimentations de vote électronique peuvent être menées dans le but de tester la faisabilité d'un système technique, elles ne sauraient être utilement envisagées, au regard des valeurs énumérées par l'article premier de la loi du 6 janvier 1978 *(« l'informatique 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 »)* que si les modalités de leur mise en œuvre ne sont pas de nature à porter une atteinte

caractérisée aux principes généraux du droit électoral qui doivent commander les opérations électorales.

Conformément aux dispositions de l'article L. 513-9 du Code du travail, ces principes s'appliquent aux élections prud'homales, y compris lorsqu'elles sont organisées par correspondance.

À cet égard, la garantie du secret du suffrage constitue un principe fondamental que seuls le caractère personnel et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du scrutin et le contrôle a *posteriori* par le juge de l'élection peuvent assurer.

Il ressort des éléments techniques fournis dans les documents joints à la demande d'avis que le dispositif retenu reposerait, d'une part, sur l'enregistrement des identifiants des électeurs et de leur bulletin de vote virtuel au sein d'un seul et même fichier faisant office d'urne virtuelle et, d'autre part, sur le recours à un procédé de chiffrement du bulletin de vote faisant appel à un algorithme de cryptologie.

La Commission considère à cet égard que les modalités de fonctionnement de ce dispositif, telles que décrites dans la demande d'avis, ne lui donnent pas, en l'état, l'assurance que ce procédé garantit effectivement le secret du suffrage et en particulier empêche que les scrutateurs ou les administrateurs du système connaissent le sens de l'expression du vote d'un électeur donné, la mairie d'Issy-les-Moulineaux admettant elle-même que *« le projet CyberVote, dans sa forme actuelle, ne garantit pas la haute confidentialité des fichiers utilisés »*.

Par ces motifs, émet un avis défavorable au projet d'arrêté présenté par la mairie d'Issy-les-Moulineaux.

Économie

Délibération n° 02-093 du 28 novembre 2002 portant avis sur le projet de loi relatif à l'économie numérique

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre délégué à l'Industrie, le 18 novembre 2002, du projet de loi relatif à l'économie numérique ;

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

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

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

Vu la directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

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

Après avoir entendu Madame Cécile Alvergnat, en son rapport et Madame Charlotte Marie Pitrat, commissaire du Gouvernement en ses observations ;

Émet l'avis suivant :

Le projet de loi relatif à l'économie numérique qui vise principalement à transposer la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique[1] reprend largement les dispositions du projet de loi sur la société de l'information (LSI) sur lequel la Commission s'était déjà prononcée par une délibération n° 01-018 portant avis en date du 3 mai 2001 rendue publique le 13 juin 2002.

Ce projet de loi établit un cadre juridique concernant des enjeux qui ont fait l'objet de nombreux débats, en particulier ceux relatifs à la prospection électronique, compte tenu notamment de la multiplicité des textes européens en la matière. Il assure en particulier la transposition des dispositions de la directive européenne du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive dite « vie privée et communications électroniques ») qui subordonnent l'utilisation de courriers électroniques dans les opérations de prospection directe au consentement préalable des personnes concernées.

Or, précisément, dans le cadre de son rapport public, *Opération boîte à spams : les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées,* adopté le 24 octobre 2002, la Commission avait appelé l'attention des pouvoirs publics sur le bénéfice que pourrait retirer l'ensemble des internautes d'une rapide transposition des dispositions concernant la prospection

[1] Directive n° 2000/31 /CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »).

par voie électronique, afin de mieux pouvoir lutter contre les émetteurs de messages électroniques non sollicités.

Observations générales :

Le texte dont la Commission est saisie s'attache notamment à compléter le dispositif relatif aux conditions de mise en jeu de la responsabilité civile et pénale des intermédiaires techniques de l'internet, à définir des règles dans le domaine du commerce électronique en encadrant notamment la publicité en ligne et enfin, à améliorer la sécurité des transactions sur internet, notamment par la libéralisation de la cryptologie.

S'agissant du régime juridique relatif à la responsabilité des prestataires techniques de l'Internet (articles 2 à 4 du chapitre II titre I « De la liberté de communication en ligne » du projet de loi)

La Commission relève que l'article 2 du projet de loi reprend notamment l'article 43-9 de la loi du 30 septembre 1986 introduit par la loi du 1er août 2000 qui établit à la charge des hébergeurs de sites mais aussi des fournisseurs d'accès à internet une obligation générale de « *détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu »,* dans les conditions et pour une durée qui doivent être précisées par un décret en Conseil d'État pris après avis de la CNIL.

La Commission regrette que plus de deux ans après l'adoption de l'article 43-9, le décret n'ait pas encore été pris, cette situation entretenant une insécurité juridique pour les prestataires techniques de l'internet.

Si la Commission n'a pas à prendre position dans le débat sur la détermination du régime de responsabilité le plus adéquat applicable aux prestataires techniques de l'internet, la question de l'identification des auteurs de contenus diffusés sur internet relève directement du domaine de la protection des données personnelles dans la mesure où ce dispositif impose très précisément aux prestataires de l'internet de mettre en œuvre des traitements permettant l'identification des auteurs de ces contenus. La Commission se réserve d'examiner cet aspect lorsqu'elle sera saisie du décret mentionné ci-dessus.

S'agissant des dispositions relatives aux contrats par voie électronique (articles 14 à 16 du chapitre III, titre II « Du commerce électronique » du projet de loi) et des dispositions relatives à la liberté d'utilisation des moyens et des prestations de la cryptologie (articles 17 à 27 du chapitre I, titre III « De la sécurité dans l'économie numérique » du projet de loi)

La Commission approuve, comme elle l'avait fait dans son avis sur le projet de loi sur la société de l'information, le principe de la liberté d'utilisation des moyens de cryptologie, de telles mesures étant incontestablement décisives pour assurer la sécurité des traitements effectués sur internet, conformément au principe de sécurité prévu à l'article 29 de la loi du 6 janvier 1978.

Par ailleurs, s'agissant des dispositions relatives aux contrats par voie électronique introduites dans le projet de loi, la Commission prend note de ce qu'elles visent à renforcer les mécanismes de protection des consommateurs.

Les observations de la Commission porteront donc principalement sur le nouveau dispositif relatif à la publicité par voie électronique.

Sur la publicité par voie électronique

Le titre II du projet de loi sur l'économie numérique consacre son chapitre II à « La publicité par voie électronique ».

L'apport principal de ce chapitre est la modification de l'article L. 33-4-1 du Code des postes et télécommunications pour assurer la transposition de l'article 13 de la directive « vie privée et communications électroniques » du 12 juillet 2002. Le nouveau texte de cet article pose le principe du consentement préalable *(opt in)* en matière de prospection directe opérée par systèmes automatisés d'appel (automates d'appel), télécopieurs ou courriers électroniques.

Le principe du consentement préalable est une garantie forte en termes de protection des personnes dont il convient de ne pas amoindrir la portée. À cet égard, la définition du « consentement »[1] issu de la directive cadre 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 exclut que l'expression de ce consentement soit, par exemple, diluée dans une acceptation des conditions générales d'utilisation d'un service proposé ou encore couplée à une demande de bons de réduction. La Commission recommande donc que le recueil du consentement soit effectué de manière à respecter le texte et l'esprit de la directive cadre de 1995, par exemple, par le biais d'une case à cocher comme le suggère l'un des considérants de la directive du 12 juillet 2002.

Observations sur le dispositif d'ensemble

Le projet de loi pose le principe du consentement préalable en matière de prospection par voie électronique au bénéfice des personnes physiques et morales. Ce choix est de nature à éviter la délicate opération qui consisterait à distinguer les adresses électroniques des personnes physiques de celles des personnes morales. En tout état de cause, la Commission a, de façon constante, considéré qu'une adresse électronique est toujours rattachée à une personne physique puisqu'elle est directement nominative lorsque le nom de la personne figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Dans le même esprit, l'abrogation de l'article L. 121-20-5 du Code de la consommation relatif à la prospection par télécopie et automates d'appel dont le champ d'application différait de l'ancien article L. 33-4-1 du Code des postes et télécommunications permet d'unifier le principe du consentement préalable à l'ensemble des personnes physiques et morales.

Cependant, le nouveau dispositif arrêté par le projet de loi appelle les réserves suivantes.

Sur la notion de courrier électronique

1) Si les notions *d'automates d'appel* et de *télécopieurs* sont claires, il importe de définir précisément celle de *courrier électronique.* En effet, l'évolution rapide des technologies impose une définition de cette notion pour lui permettre, à l'avenir, d'englober les futurs modes de communication.

L'article 2 de la directive « vie privée et communications électroniques » définit dans cette optique le « courrier électronique » comme « *tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère ».* Sont donc inclus dans cette définition les SMS et les MMS.

[1] Article 2 de la directive du 24 octobre 1995 : *« "consentement de la personne concernée" : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Le texte du projet de loi ou, à défaut, le décret en Conseil d'État prévu au 5e alinéa du nouvel article L. 33-4-1 qui doit préciser les conditions d'application de cet article devraient, dès lors, reprendre la définition issue de l'article 2 de la directive.

2) L'article 12, comme il l'a été relevé ci-dessus, modifie le Code des postes et télécommunications en y introduisant un principe général de consentement préa lable pour l'utilisation de certains moyens à des fins de prospection directe, notam ment les courriers électroniques, à l'exception notable des courriers électroniques envoyés dans le cadre de la dérogation prévue à l'alinéa 2 de l'article L. 33-4-1 du Code des postes et télécommunications. L'article 11 du projet de loi introduit, quant à lui, dans le Code de la consommation, un article L. 121-15-1 qui énonce dans son premier alinéa : « *Les publicités* non *sollicitées, notamment les* offres *promotionnel les, telles que les rabais, les primes ou les cadeaux ainsi que les concours ou les jeux promotionnels, adressées par courrier électronique, doivent-pouvoir être identifiées de manière claire et non équivoque dès leur réception par leur destinataire ».*

Il convient, dès lors, de supprimer le terme de « non *sollicitées »* de l'article L. 121-15-1 du Code de la consommation précité afin de faire peser l'obligation d'identification ainsi créée sur l'ensemble des courriers électroniques qui peuvent être reçus par une personne, que ces courriers soient sollicités (principe général du consentement préalable) ou non (exception prévue à l'alinéa 2 précité).

3) Dans la même optique, il conviendrait de clarifier la rédaction de l'alinéa 3 de l'article L. 33-4-1 du Code des postes et télécommunications qui, entre autres, transpose le premier alinéa de l'article 7 de la directive sur le commerce électro nique. En effet, dans sa rédaction actuelle, cette disposition pourrait laisser croire qu'il est possible de dissimuler l'identité de l'expéditeur ou d'envoyer un courrier électronique dont l'objet est sans rapport avec le service proposé à condition d'offrir la possibilité de s'opposer aux envois ultérieurs de tels messages.

Les interdictions posées par cet article devraient donc être plus clairement définies et s'appliquer à l'ensemble des moyens de prospection directe.

Sur le principe de la dérogation au consentement préalable en matière de prospection directe par courrier électronique

Le deuxième alinéa du nouvel article L. 33-4-1 du Code des postes et télé-communications prévoit, conformément à la directive du 1 2 juillet 2002, une dérogation au principe de recueil du consentement préalable d'une personne physique ou morale avant de lui adresser un courrier électronique à des fins de prospection directe.

1) La rédaction de cet article atteste que les conditions dans lesquelles une telle opération de prospection est possible ont été sensiblement élargies par rapport au texte communautaire. En effet, alors que la directive ne prévoyait la possibilité d'utiliser les coordonnées du destinataire que si celles-ci avaient été fournies directement dans le cadre « *d'une vente d'un produit ou d'un service »,* le projet de loi étend cette possibilité à *« la vente ou la fourniture d'une prestation de service ».*

Cette rédaction sensiblement différente permet de faire bénéficier de cette dérogation, non plus uniquement le secteur marchand — seul concerné par le terme *« vente »* issu de la directive —, mais aussi la sphère non marchande, c'est-à-dire toute personne physique ou morale qui aura fourni *« une prestation de service* ». Peuvent être considérées comme telle, par exemple, la fourniture par un site culturel d'une lettre d'information électronique à titre gratuit, l'inscription à un site, etc. Peuvent ainsi être concernés par cette dérogation, les secteurs associatifs, caritatifs voire même les personnes physiques, dès lors qu'elles fournissent une *« prestation de service ».*

En conséquence, la transposition du deuxième alinéa de l'article 13 de la directive est rédigée dans des termes qui permettent une interprétation plus large que celle issue de la lecture de la directive. En effet, le considérant 41 de la directive montre clairement le champ d'application qu'a entendu lui donner le législateur européen en énonçant : *« Dans le cadre d'une relation client-fournisseur existante, il est raisonnable d'autoriser l'entreprise qui, conformément à la directive n° 95/46/CE, a obtenu les coordonnées électroniques, et exclusivement celle-ci, à exploiter ces coordonnées électroniques pour proposer au client des produits ou services similaires... ».*

La Commission est donc réservée sur la rédaction retenue par le projet de loi qui élargit nettement le champ d'application de l'exception au principe du consentement préalable et, par là même, amoindrit la protection de la vie privée et de la tranquillité de chacun, instaurée par la directive.

2) Une opération de prospection directe effectuée dans le cadre de cette dérogation ne doit exclusivement porter, selon l'article L. 33-4-1 nouveau, que sur *« des biens ou services analogues à ceux fournis antérieurement ».* Cette rédaction, qui est celle du texte de la directive, sera inévitablement source de contentieux. Il paraît délicat, en effet, de définir a *priori* le champ exact de la notion de « biens ou services analogues », chaque entreprise pouvant alors être amenée à interpréter différemment celle-ci. À titre d'exemple, l'opération qui consiste à acheter en ligne un livre autorise-t-elle le vendeur à prospecter l'acheteur pour un disque (un disque est-il un « bien » analogue à un livre ?) ou pour un voyage (acheter un voyage en ligne est-ce un « service » analogue à l'opération d'acheter un livre en ligne ?) ? Les interprétations divergentes ne manqueront pas, au détriment, d'une part, de la sécurité juridique et, d'autre part, de la protection des données personnelles des individus, avant l'établissement d'une jurisprudence.

Nonobstant cette difficulté d'interprétation, la Commission recommande que l'article L. 33-4-1 du Code des postes et télécommunications reprenne les termes exacts de l'article 13 de la directive du 12 juillet 2002 dont le régime dérogatoire devra être entendu de manière stricte, sous peine de voir la prospection directe par courrier électronique rester dans un régime de droit d'opposition.

Dans cette même optique, il serait souhaitable que soient définies les conditions d'un régime transitoire permettant aux entreprises ayant collecté loyalement, sous le régime légal précédent, les coordonnées électroniques de clients ou de prospects d'offrir à ces derniers la faculté d'exprimer leur consentement à de futures opérations de prospection directe.

Enfin, il conviendrait que le décret en Conseil d'État prévu au 5^{e} alinéa du nouvel article L. 33-4-1 du Code des postes et télécommunications prévoie les sanctions pénales destinées à réprimer l'inobservation de ces principes et soit soumis, pour avis, à la Commission nationale de l'informatique et des libertés. L'instauration d'une amende — sanction prévue pour les contraventions de 5^{e} classe — par adresse irrégulièrement collectée paraît, en effet, une sanction plus adaptée et plus dissuasive que les dispositions générales de l'article 226-18 du Code pénal.

Enseignement

Délibération n° 02-069 du 15 octobre 2002 portant avis sur le projet d'arrêté présenté par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche concernant la modification du traitement SCOLARITÉ

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche, en application de l'article 15 de la loi du 6 janvier *)* 978, d'un projet d'arrêté portant modification du traitement dénommé SCOLARITÉ ;

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

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

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

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

Vu l'arrêté du 22 septembre 1995, modifié, portant création d'un traitement automatisé d'informations nominatives relatif au pilotage et à la gestion des élèves du second degré portant sur les trois niveaux (établissement, académie, administration centrale) ;

Vu le projet d'arrêté portant modification du traitement SCOLARITÉ présenté par le ministre de la Jeunesse, de l'Éducation nationale et de la Recherche ;

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

Formule les observations suivantes :

Le traitement SCOLARITÉ a pour objet d'assurer la gestion administrative, pédagogique et financière des élèves par les établissements publics d'enseignement du second degré, la gestion académique et l'établissement de statistiques par les rectorats et les directions départementales des services de l'éducation nationale, la gestion prévisionnelle et la mise en oeuvre d'études statistiques par l'administration centrale. 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.

La première modification dont est saisie la Commission vise à modifier l'article 5b de l'arrêté susvisé de 1995, pour intégrer dans la base élèves académique, les informations relatives à l'adresse et à la commune de résidence de l'élève et de son responsable, provenant de la base élèves établissement (BEE). La connaissance de ces informations doit permettre de réaliser d'une part, des études statistiques sur les migrations des élèves et les déplacements domicile-école en vue de l'élaboration de la carte scolaire, d'autre part des enquêtes locales. La remontée de cette information est pertinente au regard de la finalité du traitement.

La seconde modification envisagée concerne l'article 6 de l'arrêté initial et a pour objet d'autoriser les services statistiques des rectorats et la direction de la programmation et du développement, service statistique de l'administration centrale à conserver, dans leur base respective, les données pendant une durée n'excédant pas dix ans à compter de la date de leur recueil. Cette durée de conservation est justifiée par la nécessité d'évaluer à moyen et long terme les politiques éducatives mises en œuvre. Les travaux qui seront ainsi réalisés s'inscrivent dans le cadre défini par la loi du 7 juin 1951. Ce délai est pertinent au regard de la finalité poursuivie.

La troisième modification vise à intégrer, au titre des destinataires de la base académique (article 7b de l'arrêté 95), les directeurs des centres de formation d'apprentis pour les élèves entrant dans leur établissement. Les données transmises seront l'identifiant national élève (INE), le numéro de l'établissement fréquenté l'année précédente, les deux dernières classes fréquentées. Cette communication de données s'inscrit dans la mise en place d'un nouveau système d'information sur les formations des apprentis (SIFA), commun aux ministères de l'Agriculture et de l'Éducation nationale. Dans cette perspective, elle apparaît pertinente au regard de la finalité du traitement.

En outre, l'identifiant attribué à chaque élève par le ministère sera désormais dénommé « identifiant national élève » (INE).

Dans ces conditions, la Commission **émet un avis favorable** au projet d'arrêté portant modification du traitement SCOLARITÉ.

Fiscalité

Délibération n° 02-010 du 7 mars 2002 concernant la mise à la disposition des particuliers et des agents des administrations fiscales d'un service de consultation des dossiers fiscaux en ligne et la pérennisation de la procédure de transmission par internet des déclarations annuelles de revenus

La Commission nationale de l'informatique et des libertés ;
Saisie pour avis par le ministère de l'Économie, des Finances et de l'Industrie

— d'un projet d'arrêté portant création, par la direction générale des impôts, du traite ment automatisé de la transmission, par voie électronique, des éléments déclaratifs en matière d'impôt sur les revenus et portant conventions types relatives à ces opérations ;
— d'un projet d'arrêté portant création par la direction générale des impôts du trai tement automatisé dénommé « Accès au dossier fiscal des particuliers — ADONIS » ;
— de quatre projets d'arrêtés modificatifs modifiant respectivement les arrêtés du 25 juillet 1988 relatif à l'informatisation des inspections d'assiette et de documenta tion (traitement « ILIAD »), du 5 janvier 1990 relatif au traitement d'impôt sur le reve nu (« IR »), du 5 janvier 1990 relatif au système de gestion de l'identité et des adresses des contribuables (« FIP ») et du 8 mars 1996 régissant le traitement de la taxe d'habitation (« TH ») ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 31, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

Vu le Code général des impôts, notamment les articles 170-1 bis, 200 nouveau, 1649 quater B bis et 1649 quater B ter ;

Vu la délibération n° 01-008 du 8 février 2001 concernant les modifications apportées en 2001 par la direction générale des impôts à la procédure, mise en place à titre provisoire, de transmission par Internet des déclarations de revenus ;

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

Formule les observations suivantes :

Sur le projet d'arrêté portant création d'un dispositif de transmission par voie électronique des éléments déclaratifs en matière d'impôt sur le revenu

Ce nouveau traitement a pour objet de pérenniser la possibilité proposée par l'administration aux contribuables depuis l'an 2000 de déclarer leurs revenus *via* internet.

Sa mise en œuvre repose sur l'adhésion du déclarant aux clauses d'un contrat type qui définissent les conditions dans lesquelles sont garanties l'identification

de l'auteur de l'acte ainsi que l'intégrité, la confidentialité, l'opposabilité et la conservation de chaque transmission. Il énumère notamment les engagements pris par l'administration à ces différents titres.

En ce qui concerne la délivrance du certificat électronique et l'identification du contribuable

Se distinguant fortement des expérimentations menées précédemment par la Direction générale des impôts (DGI), le dispositif prévu comporte la mise en oeuvre d'une signature électronique dans le cadre d'une architecture à clés asymétriques. Pour recevoir un certificat électronique, le contribuable s'identifie préalablement en transmettant plusieurs données à caractère personnel qui figurent sur l'exemplaire papier de sa déclaration de revenus reçu pour l'année en cours ou sur le dernier avis d'imposition établi à son nom au titre de l'année précédente.

Un couple de clés est directement généré sur le poste du contribuable au moment où celui-ci s'identifie dans les conditions précitées. La clé privée du contribuable reste placée sous sa responsabilité et ne peut *être* utilisée qu'assortie d'un mot de passe choisi par lui.

Sa clé publique est transmise à la DGI qui, intervenant en qualité d'autorité d'enregistrement et de certification, l'authentifie à l'aide de sa propre clé privée. Le certificat électronique du contribuable est créé et lui est délivré en ligne, sans délai et gratuitement. Il permettra, à l'exclusion de toute autre utilisation, à l'administration des impôts de vérifier la signature des déclarations de revenus et à son détenteur de s'identifier dans le cadre du service de consultation du dossier fiscal par internet.

La Commission constate que l'ensemble du dispositif assure le niveau élevé de fiabilité des procédures de télédéclaration qui avait été souhaité par elle.

Elle estime cependant que cette procédure serait encore mieux sécurisée si l'attention des usagers était spécialement appelée sur la nécessité pour eux de préserver la confidentialité de l'un au moins des éléments à caractère personnel utilisés lors de la phase d'identification préalable du contribuable.

Cet élément d'identification dont il conviendrait de préserver spécialement la confidentialité, semble devoir être le « numéro de télédéclarant » qui, d'ores et déjà, est changé chaque année et ne figure que sur l'exemplaire papier du formulaire de déclaration de revenus de l'année. A cet effet, une mention pourrait faire apparaître qu'en cas de communication de ce document à un tiers, le numéro de télédéclarant devra être occulté.

Dans le cas de contribuables faisant l'objet d'une imposition commune, chacun d'eux peut demander à utiliser les téléservices et à recevoir un certificat électronique.

Le contrat auquel adhère le contribuable précise que la signature électronique, associée au certificat, emporte les mêmes conséquences qu'une signature manuscrite du document papier correspondant.

En ce *qui concerne les informations télétransmises, leur collecte et leur communication*

Peuvent être transmises par voie électronique la déclaration d'ensemble des revenus ainsi que les déclarations annexes, après pré-affichage à l'écran des éléments inscrits sur la déclaration papier. En cas de souscription d'une nouvelle déclaration, sur internet ou sur support papier, celle-ci est considérée comme déclaration rectificative. Ainsi, le contribuable n'est jamais obligé de recourir à la voie électronique pour faire parvenir sa déclaration.

En ce qui concerne les contribuables qui font l'objet d'une imposition commune (pour 2002, il s'agit des seuls couples mariés), la Commission rappelle une

nouvelle fois que l'article 170-1 bis du Code général des impôts dispose que *« les époux doivent conjointement signer la déclaration d'ensemble des revenus de leur foyer. »* En conséquence, seule la mise en place d'une télédéclaration assortie de deux signatures électroniques permettrait à l'administration de se conformer à l'exigence d'engagement des deux époux et ainsi de respecter les dispositions légales.

La Commission souhaite que les réflexions en cours sur ce point aboutissent rapidement et prend acte des engagements pris par l'administration sur ce sujet. Elle souhaite qu'une solution soit trouvée en 2003 au plus tard.

Afin d'assurer la confidentialité des informations transmises par voie électronique et d'éviter toute utilisation détournée de celles-ci, l'administration s'engage à ce que la totalité des transferts d'informations vers son serveur, lors des phases de saisie de la déclaration et d'envoi de la déclaration signée, s'effectue en mode sécurisé et chiffré (protocole SSLv3, clé de chiffrement de 128 bits).

Après vérification que les fichiers transmis ont été correctement reçus et que la signature électronique de la déclaration correspond à celle du déclarant, l'administration délivre en ligne, sans délai, un accusé de réception comportant notamment les éléments d'identification du contribuable, les date et heure de réception de la déclaration (heure de Paris), le numéro d'accusé de réception ainsi que la liste des documents reçus et acceptés. L'accusé de réception peut être imprimé ou téléchargé, son numéro étant nécessaire en cas de contestation ultérieure du dépôt.

En cas de non-conformité de la déclaration électronique, le contribuable est informé de l'échec de la transmission et invité à déposer une nouvelle déclaration sous forme papier ou dématérialisée.

Outre les informations portées sur les déclarations d'ensemble des revenus et relatives à l'identification des membres du foyer fiscal, à leurs revenus et à leurs charges qui sont habituellement enregistrées en mémoire informatique dans les centres des impôts, la « Télédéclaration IR » prévoit le recueil et la conservation sur support informatique d'informations complémentaires :

— les données portées sur les déclarations annexées à la déclaration d'ensemble en présence de certaines catégories de revenus ;

— pendant quinze jours, les données figurant sur les déclarations en cours de saisie ;

— les données littérales de la déclaration d'ensemble, telles que les références des établissements scolaires ou universitaires fréquentés par les enfants à charge et leur niveau d'études, le détail des frais réels ou les nom et adresse des tiers (ex. : salariés employés à domicile, assistantes maternelles, bénéficiaires de pensions alimentaires, entrepreneurs) bénéficiaires de versements déclarés au titre des charges ;

— les données littérales ajoutées sur la déclaration électronique en contrepartie de la suppression de certaines pièces justificatives : nom des organismes bénéficiaires de dons, legs ou cotisations ouvrant droit à réduction d'impôt — à l'exception de ceux des organisations syndicales, des associations cultuelles ou de bienfaisance et, lorsque leur montant est inférieur ou égal à 3 000 euros, des associations de financement électoral, partis et groupements politiques —, montant total des versements effectués à chacun d'entre eux.

La Commission constate qu'en dépit des précautions prises par le législateur, il ne peut être exclu que le nom des organismes bénéficiaires de dons Fasse apparaître indirectement notamment les opinions politiques, philosophiques ou religieuses des contribuables et qu'ainsi il constitue une information dont l'enregistrement et la conservation ne sont normalement envisagés, en application de l'article 31 de la loi du 6 janvier 1978, qu'avec l'accord exprès de l'intéressé ou, pour des

motifs d'intérêt public, par décret en Conseil d'État pris sur proposition ou avis conforme de la CNIL.

Toutefois, la Commission considère qu'un tel décret n'est pas nécessaire dès lors que :

— s'agissanf de la collecte et de l'enregistrement des informations en cause, le décret ne pourrait que reprendre les termes de la loi ;

— s'agissant des modalités de leur conservation et de leur utilisation, le projet d'arrêté relatif au traitement « ADONIS » prévoit, à l'issue de l'instruction du dos sier, que ces informations ne sont pas conservées dans « ADONIS » au-delà de six mois — c'est-à-dire le temps nécessaire pour permettre à l'administration d'atteindre l'objectif voulu par le législateur — et que tout traitement spécifique à partir de ces données est rendu techniquement impossible.

En ce qui concerne la conservation des informations transmises

Afin de garantir l'opposabilité des données reçues par la DGI, l'ensemble des informations transmises (déclarations de revenus signées avec leurs annexes, date et heure des dépôts, données relatives à la certification des envois) sont conservées, chiffrées et signées, pendant dix ans à compter de l'année d'imposition dans une base d'archivage afin de permettre, en cas de contestation du contribuable, la vérification de la signature et du contenu d'une transmission. Ces informations, qui sont intangibles, sont opposables au contribuable et à l'administration. Leur vérification peut être effectuée devant un expert nommé par les tribunaux.

Sur le projet d'arrêté portant création de la base nationale de consultation « ADONIS »

Ce traitement a pour objet principal la mise en place d'un service de consultation en ligne des dossiers nominatifs de fiscalité personnelle des contribuables.

En ce qui concerne le contenu de la base

« ADONIS » comporte, pour chaque foyer fiscal :

— les déclarations d'ensemble des revenus et les déclarations annexes transmises par voie électronique, les date et heure du dépôt des déclarations, le numéro des accusés de réception électroniques ;

— les éléments des déclarations d'ensemble des revenus reçues sur support papier, lorsqu'ils sont conservés sur support informatique par l'administration ;

— les avis d'imposition concernant l'impôt sur le revenu, les contributions sociales (CSG, CRDS), la taxe d'habitation et les taxes foncières ;

— une présentation synthétique du dossier fiscal du contribuable et un résumé de chaque imposition ;

— des informations relatives aux réclamations, aux impositions supplémentaires émises ainsi qu'aux dégrèvements.

Ces informations sont mises à la disposition de l'ensemble des utilisateurs d'ADONIS dans les mêmes conditions et pendant les mêmes durées de conservation, sous réserve des précisions ci-après.

En ce *qui concerne la consultation de la base par les contribuables*

Pour avoir accès, *via* internet, à son dossier fiscal mis en ligne, chaque contribuable s'authentifie en transmettant le certificat électronique en cours de validité qui lui a été précédemment délivré par la DGI ou dont il obtient la délivrance en suivant la procédure d'identification préalable prévue pour la télédéclaration des revenus. Il ne peut accéder qu'aux informations conservées dans son dossier fiscal.

L'administration met en œuvre un cryptage des données téléconsultées suivant le protocole SSLv3 (clé de chiffrement de 128 bits).

La Commission constate que ce dispositif assure un niveau de sécurisation du téléservice de consultation du dossier fiscal qui, en l'état actuel de la technologie, peut être jugé satisfaisant.

Par ailleurs, la Commission attire l'attention de l'administration sur les dispositions de l'article 35 de la loi du 6 janvier 1978 et sur les termes de sa délibération n° 80-10 du 1er avril 1980 qui impliquent que toutes les informations conservées dans la base, et donc consultables par les contribuables, puissent l'être sous une forme directement compréhensible par eux et donc non codée.

Enfin, la Commission rappelle que le ministère de l'Economie, des Finances et de l'Industrie prévoit de mettre en place, à terme, d'autres dispositifs de consultation des mêmes informations (serveur vocal, bornes publiques de consultation du site du ministère...) afin d'éviter toute « fracture numérique » dans la société. Elle exprime le souhait que ces services soient développés dans les meilleurs délais.

En ce qui concerne la consultation de la base par les agents des administrations fiscales

La consultation de la base « ADONIS » sera en principe ouverte, *via* l'intranet ministériel, à tous les agents de la DGI et de la Direction générale de la comptabilité publique (DGCP), sous réserve que ces agents aient à l'égard des contribuables dont les dossiers sont consultés une mission d'assiette, de contrôle ou de recouvrement en matière fiscale.

D'une part, un contrôle a priori des accès au traitement est mis en œuvre par l'intermédiaire d'un annuaire qui recense non pas des habilitations individuelles, fonction des attributions géographiques et fonctionnelles précises des agents, mais de « profils applicatifs » plus larges, à caractère géographique. Trois niveaux d'accès à « ADONIS » sont ainsi prévus :

— un niveau national, pour des agents ayant une compétence nationale (bureaux d'administration centrale, directions nationales à compétence spécialisée) et cer tains agents des directions des services fiscaux et des trésoreries générales ;

— un niveau inter régional, pour certains agents des directions du contrôle fiscal et des trésoreries générales ;

— un niveau départemental pour les autres agents habilités des services déconcen trés de la DGI et de la DGCP (ex. : centres des impôts, trésoreries), étant entendu qu'un agent accède à l'ensemble des données contenues dans les dossiers fiscaux qui comportent au moins une occurrence fiscale située dans son département d'exercice.

En outre, certains dossiers, qualifiés de sensibles par l'administration, feront l'objet d'une protection renforcée de leur confidentialité : seuls quelques agents bénéficiant d'une habilitation supérieure pourront y accéder.

D'autre part, un contrôle a *posteriori* de la bonne application de la règle de consultation est permis grâce à un dispositif de journalisation des consultations par les agents des dossiers fiscaux et de conservation des données correspondantes pendant un an.

La Commission prend acte de ce dispositif. Elle estime qu'ainsi conçu, il n'assurera la nécessaire protection des données à caractère personnel et du secret fiscal qu'au prix d'une grande exigence dans l'application des contrôles a posteriori qui sont envisagés.

À cet égard, la Commission estime qu'il serait utile de prévoir un contrôle a posteriori *aléatoire qui devrait concerner au moins 1 % des interrogations de la base « ADONIS ».*

En ce qui concerne l'utilisation des informations contenues dans la base
La DGI souhaite être autorisée à utiliser les informations d'identification des contribuables pour mener des enquêtes-qualité sur les téléprocédures fiscales. Elle reconnaît cependant aux intéressés le droit de s'opposer à faire l'objet de ces sollicitations, en application de l'article 26 de la loi du 6 janvier 1978.

La Commission estime qu'indépendamment de l'information assurée par l'arrêté portant création du traitement « ADONIS », il convient que les usagers de ce traitement soient informés du droit d'opposition qui leur est reconnu selon des modalités qui en facilitent l'exercice.

Au bénéfice des observations qui précèdent, la Commission émet un, avis favorable sur les projets d'arrêtés qui lui sont présentés par le ministère de l'Economie, des Finances et de l'Industrie.

Le présent avis est assorti de la demande de présentation d'un bilan quantitatif et qualitatif sur les conditions de mise en oeuvre en 2002 de ces traitements.

Délibération n° 02-092 du 28 novembre 2002 concernant la modification de plusieurs traitements d'informations nominatives mis en oeuvre par la Direction générale des impôts et certains aménagements dans les relations avec les contribuables résultant de l'entrée en vigueur des dispositions fiscales de la loi relative au PACS

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Economie, des Finances et de l'Industrie de huit projets d'arrêtés modifiant les traitements automatisés dénommés « MAJIC 2 », « FIP », « SIR », « ILIAD », « ISF », « IR », « TH » et « ADONIS » et destinés à permettre la prise en compte des conséquences fiscales du pacte civil de solidarité ;

Vu la directive n° 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 ;

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 les articles 29 et 31, ensemble le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des dispositions de la loi précitée ;

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

Vu le Code général des impôts, notamment les articles 6, 7, 1379 bis, 1685 bis et 1723 ter ;

Vu les articles L. 111, L. 253 et R. 111-1 et suivants du Livre des procédures fiscales ;

Vu la loi n° 99-944 du 15 novembre 1999 relative au pacte civil de solidarité, ensemble la décision du Conseil constitutionnel n° 99-419 du 9 novembre 1999 ;

Vu le décret n° 99-1090 du 21 décembre 1999 relatif aux conditions dans lesquelles sont traitées et conservées les informations relatives à la formation, la modification et la dissolution du pacte civil de solidarité et autorisant la création à cet effet d'un traitement automatisé des registres mis en oeuvre par les greffes des tribunaux d'instance, par le greffe du tribunal de grande instance de Paris et par les agents diplomatiques et consulaires français ;

Vu le décret n° 99-1091 du 21 décembre 1999 portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 à l'enregistrement et à la conservation des informations nominatives relatives à la formation, la modification et la dissolution du pacte civil de solidarité, notamment son article 3 ;

Vu les lettres en date des 13 mai et 1er août 2002 du Direction général des impôts au président de la CNIL concernant différents aménagements à prévoir dans les relations de l'administration avec les contribuables pour tenir compte de l'imposition commune des personnes liées par un PACS ;

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

Formule les observations suivantes :

L'article 6-1 du Code général des impôts prévoit que les partenaires liés par un pacte civil de solidarité (PACS) font l'objet, pour le calcul de l'impôt sur le revenu, d'une imposition commune à compter de l'imposition des revenus de l'année du troisième anniversaire de l'enregistrement du pacte. Cette mesure entre en application pour les personnes ayant conclu un PACS fin 1999 à compter des revenus perçus en 2002, déclarés en 2003.

Sur les projets d'arrêtés modificatifs soumis à l'avis de la Commission

1) Les projets d'arrêtés transmis à la CNIL visent à permettre l'introduction dans certains traitements automatisés mis en œuvre par la Direction générale des impôts (DGI) des informations relatives aux PACS qui seront dorénavant demandées sur les formulaires de déclaration des revenus. Les catégories d'informations nominatives enregistrées sont l'existence du pacte, l'état civil des partenaires, la date de conclusion du pacte ainsi que, le cas échéant, celle de sa dissolution.

Ces informations seront enregistrées dans le traitement « ILIAD », utilisé dans les centres des impôts, dont les finalités sont la gestion de l'assiette, des impositions supplémentaires, des réclamations et des contentieux relatifs à l'impôt sur le revenu, à la taxe d'habitation, aux contributions sociales et à la taxe annuelle sur les logements vacants, ainsi que la gestion des dossiers fiscaux dématérialisés. Les mêmes informations sont conservées dans le traitement « ADONIS » qui permet aux agents des administrations fiscales et aux seuls contribuables concernés, de consulter les dossiers fiscaux des particuliers mis en ligne *via* internet.

En outre, les chaînes de traitements mises en œuvre pour la gestion des foyers fiscaux (« FIP »), de l'impôt sur. le revenu (« IR »), de la taxe d'habitation (« TH »), de l'impôt de solidarité sur la fortune (« ISF »), des taxes foncières (« MAJIC 2 ») et des informations de recoupement (« SIR/FLR ») auront communication de données relatives à l'existence d'un pacte et à l'identité des partenaires. La transmission d'informations à ces traitements a pour objet de permettre la prise en compte de l'existence des foyers fiscaux constitués du fait de l'imposition commune des revenus des signataires d'un PACS, pour la gestion des décisions d'exonération/dégrèvement des impôts locaux soumis à conditions de revenu et de cohabitation, pour la gestion de l'imposition commune à l'**ISF** des personnes liées par un pacte, ou pour le contrôle de leurs revenus.

Ces transmissions d'informations sont adéquates, pertinentes et non excessives au regard des finalités poursuivies.

2) Le décret n° 99-1091 susvisé interdit toute sélection d'une catégorie particulière de personnes à partir des informations relatives aux PACS qui relèvent des données sensibles mentionnées à l'article 31 de la loi du 6 janvier 1978.

À l'appui de chacun des projets d'arrêté soumis à la Commission, l'administration précise que le traitement, tel qu'il était modifié, ne permettait pas techniquement de sélectionner ou d'extraire des listes de partenaires d'un PACS.

Ces garanties, qui doivent également s'appliquer aux traitements que la Direction générale de la comptabilité publique (DGCP) met en œuvre pour le recouvrement des impôts directs, sont de nature à satisfaire les prescriptions du décret n° 99-1091.

3) L'administration indique également : *« Les agents qui de par leur fonction auront accès à la connaissance de la qualité de partenaire d'un pacte seront plus particulièrement rappelés à leurs obligations de secret professionnel et de discrétion ».*

La Commission prend acte de cet engagement et estime que les mêmes précautions devront être prises pour les personnels de la DGCP.

Sur les aménagements à envisager dans les relations avec les contribuables en vue de préserver la confidentialité des informations relatives au PACS

1) Pour permettre aux contribuables liés par un pacte de souscrire une déclaration commune, l'administration modifiera le formulaire de déclaration des revenus :
— en faisant figurer, à côté de la mention « conjoint », les mots « ou partenaire » ;
— en créant une nouvelle zone « situation de famille au sens fiscal » ;
— pour la prise en compte des revenus catégoriels, en remplaçant la formulation « vous/conjoint » par « vous/conjoint ou partenaire ».

Ces modalités n'appellent pas d'observation de la Commission.

2) L'article 6-1 troisième alinéa du CGI qui prévoit l'imposition commune à l'impôt sur le revenu des contribuables liés par un PACS spécifie *in fine* : *« L'imposition est établie à leurs deux noms, séparés par le mot "ou" ».* L'administration a envisagé d'adopter les mêmes principes pour l'adresse des courriers destinés aux intéressés, en utilisant le libellé « M (ou M^{me}) nom, prénom ou M (ou M^{me}) nom, prénom ».

Mais le fait de faire apparaître, en matière d'impôt sur le revenu, sur les enveloppes deux noms de contribuables pouvant désigner des individus du même sexe comporte déjà, par lui-même, un certain risque de divulgation d'informations relevant de l'article 31 de la loi du 6 janvier 1978. Ce risque paraît encore aggravé si ces noms sont reliés par la conjonction « ou » qui n'est, par ailleurs, utilisée que sur les courriers fiscaux adressés aux personnes mariées.

En conséquence, la Commission estime que devrait être ouverte aux contribuables, dans le cadre du programme COPERNIC de refonte du système d'information fiscal et dans un délai qui ne devrait pas être supérieur à cinq ans, la faculté de désigner l'un des membres du foyer fiscal comme destinataire unique des courriers de l'administration, à l'exception des courriers de procédure.

Dans l'immédiat, elle recommande, pour les correspondances adressées aux partenaires d'un PACS, l'emploi du libellé déjà utilisé en matière de taxe d'habitation ou de taxes foncières pour les impositions communes à plusieurs personnes portant des noms différents : *« M (ou M^{me}) nom, prénom et M (ou M^{me}) nom, prénom »,* comme pour les couples mariés dont l'épouse aura manifesté le souhait d'être identifiée sous son nom patronymique.

3) Les dispositions précitées de l'article 6-1 du CGI conduiront les services d'assiette à établir les avis d'imposition des contribuables liés par un PACS *« à leurs deux noms, séparés par le mot "ou" ».* Or, la copie de l'avis d'imposition sur le revenu est un document fréquemment demandé dans la vie courante — par exemple avant la conclusion d'un bail, alors que le bailleur n'est pas au nombre des tiers créanciers ayant accès aux registres de PACS. Le risque existe donc que, par le biais de la communication des avis d'imposition, se trouve amoindrie la protection voulue par le législateur et le pouvoir réglementaire des données relatives au PACS lors qu'elles révèlent des informations sensibles au sens de l'article 31 de la loi du 6 janvier 1978.

Certes, la production d'un avis d'imposition est rarement obligatoire et rien n'interdit d'occulter les mentions de l'avis qui n'intéressent pas les tiers. Mais les personnes concernées ne sont pas toujours informées de leurs droits ou en situation de les exercer.

En conséquence, la Commission souhaite qu'au titre des services accessoires susceptibles d'être offerts aux contribuables, notamment dans le cadre de l'administration électronique, soit étudiée la possibilité de remettre aux personnes qui en feraient la demande des justificatifs individuels de situation fiscale ne comportant pas l'ensemble des renseignements figurant sur les avis d'imposition, notamment de ceux relatifs à la situation familiale. Ce nouveau service présenterait un intérêt majeur pour de nombreux contribuables.

4) Les articles L. 111 et R. 111-1 et suivants du Livre des procédures fiscales (LPF) permettent à tout contribuable de prendre connaissance de l'identité, de l'adresse, du nombre de parts retenu pour l'application du quotient familial, du revenu imposable, de l'avoir fiscal et du montant de l'impôt pour l'ensemble des personnes assujetties à l'impôt sur le revenu qui relèvent de la même direction des services fiscaux.

Actuellement, les listes consultables regroupent les informations par foyer fiscal et sont classées par commune, puis par adresse, enfin par ordre alphabétique lorsque plusieurs foyers sont domiciliés à la même adresse.

Un tel dispositif rendrait aisé, s'il n'était pas aménagé, le contournement des restrictions apportées par la réglementation en vigueur à la consultation des registres de PACS.

Tenant compte des problèmes soulevés, la DGI a fait connaître que de nouvelles modalités de constitution des listes de contribuables pourraient être retenues : les informations continueraient à être présentées par foyer fiscal, sauf pour deux catégories de foyers — ceux des personnes liées par un PACS et les couples mariés dont l'épouse aura demandé à être désignée sous son nom patronymique — ; la civilité n'apparaîtrait pas sur ces listes ; seule l'initiale du prénom des personnes y serait mentionnée.

En revanche, la substitution de l'ordre alphabétique au sein de la commune — ou de l'arrondissement — au classement des contribuables par adresse n'est pas retenue par l'administration pour des raisons techniques et de coût. La Commission estime cependant que cette modalité serait, seule, de nature à donner leur plein effet aux mesures décrites ci-dessus.

Au bénéfice des observations qui précèdent, la Commission :

Émet un avis favorable sur les projets d'arrêtés modificatifs qui lui sont soumis par le ministère de l'Économie, des Finances et de l'Industrie.

Recommande :

— l'abandon de la conjonction « ou » dans les adresses des courriers envoyés, en matière d'impôt sur le revenu aux contribuables liés par un pacte civil de solidarité ;

— l'aménagement dans le sens indiqué ci-dessus des listes de contribuables à l'impôt sur le revenu prévues à l'article L. 111 du LPF.

Internet

Délibération n° 02-066 du 24 septembre 2002 portant avis sur la modification du traitement mis en œuvre dans le cadre du site internet Légifrance

La Commission nationale de l'informatique et des libertés ;

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

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

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

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration, notamment son article 2 ;

Vu le décret n° 2002-1064 du 7 août 2002 relatif au service public de la diffusion du droit par l'internet ;

Vu l'arrêté du 6 juillet 1999 relatif à la création du site internet Légifrance ;

Vu la délibération de la Commission n° 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence ;

Vu le projet d'arrêté relatif au site internet Légifrance présenté par le Premier ministre ;

Après avoir entendu M. Pierre Leclercq, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

Le site internet Légifrance, créé par un arrêté du 6 juillet 1999 pris après avis de la CNIL, avait pour vocation de diffuser gratuitement certaines données juridiques publiques pouvant revêtir un caractère nominatif. La jurisprudence des cours et tribunaux était diffusée, sous une forme payante, sur le site www.jurifrance.tm.fr

Par décret du 7 août 2002, le Gouvernement a décidé que le site Légifrance constituerait désormais le portail unique permettant l'accès gratuit aux textes en vigueur ainsi qu'à la jurisprudence.

Le site internet Légifrance est placé sous la responsabilité du secrétariat général du Gouvernement.

Il comporte des traitements automatisés d'informations nominatives ayant pour finalités la diffusion de données nominatives publiées au *Journal officiel de la République française,* la diffusion de la jurisprudence administrative et judiciaire ainsi que des décisions du Conseil constitutionnel, et la gestion du courrier électronique déposé par les usagers du site.

L'article 3 du projet d'arrêté prévoit que certaines catégories d'informations parues au *Journal officiel* sont exclues de la diffusion sur le site Légifrance. Il s'agit des décrets portant naturalisation, réintégration, mention d'enfant mineur bénéficiant de l'effet collectif attaché à l'acquisition de la nationalité française par les

parents et francisation de noms et prénoms, des décrets portant changement de nom, des décrets et arrêtés portant constatation de l'exclusion de droit de la Légion d'honneur et d'une radiation de droit des contrôles de la médaille militaire, des décrets et arrêtés portant constatation de l'exclusion de droit de l'ordre national du Mérite, des arrêts de la Cour de discipline budgétaire et financière, des décisions de sanction du Conseil de prévention et de lutte contre le dopage, des avis de la Commission des opérations de bourse relatifs à des décisions de sanction.

L'article 4 du projet d'arrêté prévoit en outre que, s'agissant des catégories d'informations nominatives figurant dans les décisions de justice, l'identité et l'adresse des parties au procès ou des témoins seront occultées des décisions mises en ligne sur le site après le 15 septembre 2002.

S'agissant des décisions de justice mises en ligne avant cette date, le secrétariat général du Gouvernement, d'une part, a pris l'engagement de procéder à l'occultation des informations nominatives concernant les parties et témoins dans un délai de deux ans et, d'autre part, a, afin de préserver la protection des données personnelles, adopté des mesures techniques entravant le transfert complet de l'ensemble des informations du site Légifrance à l'initiative des responsables d'autres sites qui prétendraient les mettre en ligne.

L'ensemble de ces mesures s'inscrit dans l'esprit des recommandations de la CNIL formulées dans sa délibération du 29 novembre 2001 portant sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence, réalisant ainsi un juste équilibre entre le caractère public des données diffusées et leur libre accessibilité sur internet.

Le droit d'accès, de rectification ainsi que le droit d'opposition s'exercent auprès de la Direction des Journaux officiels, pour ce qui concerne les documents diffusés sur le site, auprès de l'hébergeur, pour ce qui concerne la messagerie du site.

Prend acte :

— des mesures prises par le secrétariat général du Gouvernement pour, d'une part, exclure certains documents publiés au *Journal officiel de la République française* de la diffusion sur le site internet Légifrance et, d'autre part, procéder à l'occultation de l'identité et de l'adresse des parties et témoins des décisions de justice diffusées sur le site à compter du 15 septembre 2002 ;

— de l'engagement pris par le secrétariat général du Gouvernement d'occulter, dans un délai de deux ans, l'identité et de l'adresse des parties et témoins des déci sions de justice préalablement diffusées.

Émet, en conséquence, **un avis favorable** au projet d'arrêté relatif au site internet Légifrance présenté par le Premier ministre.

Justice

Délibération n° 02-072 du 24 octobre 2002 portant avis sur le projet d'arrêté du ministre de la Justice abrogeant et remplaçant l'arrêté du 28 octobre 1996 portant création d'un fichier national des personnes incarcérées

La Commission nationale de l'informatique et des libertés ;

Saisie, par le ministère de la Justice d'un projet d'arrêté abrogeant et remplaçant l'arrêté du 28 octobre 1996 portant création d'un fichier national automatisé des personnes incarcérées ;

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

Vu la 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 ensemble les articles 706-9 à 706-11 du Code de procédure pénale relatifs à l'action récursoire du fonds de garantie des victimes des actes de terrorisme et d'autres infractions et D. 113 du même Code relatif à la répartition du produit du travail des détenus ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres I^{er} à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le décret n° 86-835 du 10 juillet 1986 relatif aux modalités d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques dans les traitements automatisés concernant le ministère de la Justice ;

Vu l'article D. 287 du Code de procédure pénale ;

Vu l'arrêté du 28 octobre 1996 portant création d'un fichier national des personnes incarcérées ;

Vu les délibérations n° 89-32 et n° 89-72 de la Commission en date des 25 avril et 11 juillet 1989 ;

Après avoir entendu Monsieur Patrick Delnatte, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre de la Justice a saisi la Commission d'un projet d'arrêté portant modification du fichier national des détenus (FND), qui a pour finalité la gestion des affectations pénitentiaires des détenus, ainsi que la production de statistiques concernant la population pénale.

Les modifications envisagées portent sur la collecte et le traitement de nouvelles informations nominatives, sur la transmission par réseau d'informations extraites de l'application locale de gestion informatisée des détenus en établissement (GIDE), sur l'allongement de la durée de conservation des informations traitées à quinze mois à compter de la date de levée d'écrou et sur l'accès à ce fichier par l'intermédiaire d'un réseau intranet pour les services de la Chancellerie et par extranet sécurisé pour les utilisateurs extérieurs des ministères de l'Intérieur et de la Défense.

Sur les nouvelles catégories d'informations nominatives collectées

La Chancellerie souhaite compléter la liste des informations nominatives détaillées figurant déjà dans le FND par l'ajout de renseignements complémentaires relatifs à l'identité du détenu [commune et arrondissement de naissance (y compris ville à l'étranger), adresse à la libération, filiation (nom et prénom du père et de la mère), adresse du domicile], à sa situation familiale (nombre d'enfants en détention) et à son incarcération [catégorie administrative, détenu déjà incarcéré (sous la forme « oui/non »), nombre d'affaires, mesures d'éloignement, mouvance (sous la forme « oui/non »), indication du statut de détenu particulièrement surveillé (sous la forme « oui/non »), suivi médical (sous la forme « oui/non »), handicap (sous la forme « oui/non »), quartier d'affectation, procédure, date de première condamnation définitive, date de fin de peine, date de libération, nom du juge d'instruction, quantum de peine en cours, somme des quantums des peines, somme des remise de peine].

La collecte de ces nouvelles informations a pour objet de permettre une identification plus fiable des détenus, une prise en charge plus adaptée en établissement par une meilleure connaissance de leur situation spécifique et la production de tableaux de bord et de statistiques à partir d'éléments d'information qui ne figuraient pas dans le FND jusqu'à présent.

La Chancellerie souhaite également disposer de nouvelles catégories d'informations anonymisées enregistrées au titre de la fonction de production de statistiques (établissements par zone 1300, établissements par SRPJ, capacité norme circulaire, capacité opérationnelle).

La collecte de ces informations apparaît pertinente au regard de la finalité du traitement.

Sur l'allongement de la durée de conservation des informations traitées

La Chancellerie souhaite porter à quinze mois, à compter de la date de levée d'écrou, la durée de conservation des informations nominatives, initialement fixée jusqu'au 1er avril de l'année suivant l'année de libération.

Cet allongement poursuit un double objectif : instituer, d'une part, une durée de conservation à partir de la date de levée d'écrou des détenus en remplacement de la procédure d'archivage initiale qui intervenait à date fixe dans l'année ; harmoniser, d'autre part, les durées de conservation des informations traitées dans le FND et l'application GIDE, qui désormais alimente pour partie le FND.

La modification envisagée de cette durée de conservation n'apparaît pas excessive au regard de la finalité du traitement.

Sur les moyens d'accès au fichier

Le fichier sera accessible aux utilisateurs de la Chancellerie par l'intermédiaire de l'intranet du ministère et par extranet, au moyen d'une consultation sécurisée, pour les utilisateurs des ministères de l'Intérieur et de la Défense.

La consultation du FND s'opère au moyen de terminaux dotés de lecteurs de carte sécurisés. Les cartes à mémoire sont attribuées nominativement à chaque personne habilitée à consulter le fichier. Un code secret individuel est associé à chaque carte à mémoire. La présence de la carte à mémoire et l'indication de son code d'accès sont obligatoires pour accéder à l'application.

En outre, le FND gère le profil de chacun de ses utilisateurs ; ce profil détermine les informations auxquelles chaque utilisateur peut avoir accès.

Les mesures de sécurité et de confidentialité entourant le traitement apparaissent en conséquence adaptées au regard de sa finalité et des informations traitées.

Émet un avis favorable au projet d'arrêté du ministre de la Justice abrogeant et remplaçant l'arrêté du 28 octobre 1996 portant création d'un fichier national automatisé des personnes incarcérées.

Délibération n° 02-073 du 24 octobre 2002 portant avis sur le projet d'arrêté du ministre de la Justice abrogeant et remplaçant l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires

La Commission nationale de l'informatique et des libertés ;

Saisie, par le ministère de la Justice d'un projet d'arrêté abrogeant et remplaçant l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires ;

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

Vu la 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 ensemble les articles 724, 724-1, D. 148 à D. 166 et D. 319 à 334 du Code de procédure pénale ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application des chapitres I^{er} à IV et VII de la loi du 6 janvier 1978 précitée ;

Vu le décret n° 86-835 du 10 juillet 1986 relatif aux modalités d'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques dans les traitements automatisés concernant le ministère de la Justice ;

Vu l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires ;

Vu la délibération n° 90-91 de la Commission en date du 11 juillet 1990 ;

Après avoir entendu Monsieur Patrick Delnatte, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Formule les observations suivantes :

Le ministre de la Justice a saisi la Commission d'un projet d'arrêté abrogeant et remplaçant l'arrêté portant création de l'application de prise en charge des détenus dans les établissements pénitentiaires (PECD), qui a pour finalité la gestion des greffes pénitentiaires, des comptes nominatifs des détenus, de la détention et des visites dans les conditions prévues par les articles 724, 724-1, D. 148 à D. 166 et D. 319 à 334 du Code de procédure pénale.

La principale modification envisagée porte sur le remplacement de l'application PECD, déclarée en 1990, par une nouvelle application de gestion informatisée des détenus en établissement (GIDE) ayant la même finalité et permettant d'alimenter automatiquement, pour une partie des informations nominatives qui y sont enregistrées, le fichier national des détenus (FND).

Le ministère de la Justice entend également élargir la liste des informations soumises à la procédure de droit d'accès indirect, prévue au titre de l'article 39 de la loi du 6 janvier 1978.

Le ministère de la Justice souhaite enfin allonger de trois mois la durée de conservation des informations nominatives traitées, fixée jusqu'à présent à douze mois à compter de la date de levée d'écrou.

Sur l'alimentation du fichier national des détenus

L'application GIDE permettra d'alimenter automatiquement, sur une base quotidienne, le fichier national des détenus.

Cette alimentation ne portera que sur les informations relatives à la gestion des greffes et de la détention, telles qu'énumérées dans l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires qui a fait l'objet d'un avis favorable de la Commission par délibération n° 90-091 du 10 juillet 1990 et dans le projet d'arrêté l'abrogeant et le remplaçant.

La Commission observe que ces informations, jusqu'à présent transmises par les établissements pénitentiaires à la direction de l'administration pénitentiaire sur support papier, seront désormais communiquées par l'intermédiaire du réseau intranet sécurisé du ministère de la Justice.

Sur l'application de la procédure du droit d'accès indirect

Les informations figurant dans l'application de gestion des détenus susceptibles de relever de la procédure d'accès indirect concernent : les dates des transferts, des translations judiciaires et des extractions des détenus concernés, la désignation des locaux de visite, ainsi que, désormais, l'ensemble des informations relatives à la gestion de la détention (désignation des locaux de l'établissement, des activités proposées et de leurs horaires, description des mouvements des détenus à l'intérieur de l'établissement, désignation des personnes qui décident de l'affectation des détenus, mentions particulières relatives à certains détenus : ne pas mettre seul en cellule, ne pas mettre dans la même cellule que certains détenus, mettre seul en cellule, risque d'évasion).

La Commission estime que, dans la mesure où la communication aux intéressés de ces informations serait susceptible de porter atteinte à la sécurité publique ou à la sûreté de l'État, l'application à ces données de la procédure de droit d'accès indirect est justifiée.

Elle prend acte de ce que l'ensemble des autres informations reste soumis au droit d'accès direct et que les détenus et leur famille en sont informés par une affichette apposée dans les locaux de l'établissement.

Sur l'allongement de la durée de conservation des informations traitées

L'allongement de cette durée de conservation a pour objet de pouvoir répondre aux demandes constantes d'informations concernant des détenus libérés émanant des juridictions et des greffes pénitentiaires.

Il vise également à disposer d'une durée de conservation identique dans l'application GIDE et le FND, qu'elle alimente.

La Commission estime que l'allongement à quinze mois de la durée de conservation initialement arrêtée n'est pas excessive au regard de la finalité du traitement.

Émet un avis favorable au projet d'arrêté du ministre de la Justice abrogeant et remplaçant l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires.

Police

Délibération n° 02-008 du 7 mars 2002 portant avis sur un projet de décret modifiant le Code de procédure pénale et relatif au fichier national des empreintes génétiques

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par la garde des Sceaux, ministre de la Justice d'un projet de décret modifiant le Code de procédure pénale et relatif au fichier national des empreintes génétiques ;

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

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

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

Vu le Code pénal ;

Vu le Code de procédure pénale et notamment ses articles 706-47, 706-54, 706-55 et 706-56 ;

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° 2000-413 du 18 mai 2000 modifiant le Code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques ;

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

Formule les observations suivantes :

Le ministère de la Justice a saisi la Commission, pour avis, d'un projet de décret modifiant les dispositions du Code de procédure pénale relatives au fichier national automatisé des empreintes génétiques issues du décret n° 2000-413 du 18 mai 2000 sur lequel la Commission s'est prononcée par une délibération n° 99-052 du 28 octobre 1999.

Le projet de texte a pour objet d'étendre le champ d'application du fichier national automatisé des empreintes génétiques tel qu'il a été à nouveau défini par l'article 56 de la loi n° 2001-1062 du 15 novembre 2001 sur la sécurité quotidienne.

Aux termes de ces dispositions législatives, les infractions pouvant donner lieu à inscription dans le fichier sont celles dorénavant visées à l'article 706-55 du Code de procédure pénale qui concernent, outre les infractions de nature sexuelles visées à l'article 706-47 du Code de procédure pénale, les crimes d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie et de violences volontaires, les crimes de vol, d'extorsions et de destructions ; dégradations et détériorations dangereuses pour les personnes et les crimes constituant des actes de terrorisme.

Il est donc proposé de remplacer, aux premiers alinéas des articles R. 53-10, R. 53-20 et R. 53-21 du Code de procédure pénale issus des dispositions du décret du 18 mai 2000, la référence à l'article 706-47 par celle de l'article 706-55.

La modification proposée qui a pour seul objet d'assurer la mise en conformité des dispositions réglementaires à la loi, n'appelle pas en conséquence d'observation particulière de la Commission.

Émet un avis favorable au projet de décret présenté par la garde des Sceaux, ministre de la Justice modifiant le Code de procédure pénale et relatif au fichier national des empreintes génétiques.

Position de la CNIL du 24 octobre 2002 sur les dispositions du projet de loi pour la sécurité intérieure relatives aux fichiers de police judiciaire et au fichier national automatisé des empreintes génétiques

La Commission nationale de l'informatique et des libertés, réunie en séance plénière le 24 octobre, a examiné le projet de loi pour la sécurité intérieure qui vient d'être adopté en Conseil des ministres ;

Autorité administrative indépendante chargée par la loi du 6 janvier 1978 d'assurer la protection des données personnelles figurant dans les fichiers informatiques, la Commission se doit de faire connaître sa position sur les dispositions du projet de loi concernant de tels fichiers. Tout en regrettant de ne pas avoir été consultée lors de son élaboration, la Commission estime ainsi devoir exprimer ses principales observations sur les articles relatifs aux fichiers de police judiciaire et au fichier national automatisé des empreintes génétiques ;

Sur les fichiers de police judiciaire

1) L'existence des fichiers de police judiciaire sera désormais consacrée par la loi, ce que la CNIL avait souhaité lors de l'avis rendu en décembre 2000 sur le fichier national de police judiciaire mis en œuvre par le ministère de l'Intérieur (STIC).

Certaines garanties importantes du point de vue de la protection de la vie privée et des libertés individuelles figurent dans le projet de loi, telles celles relatives au contrôle du procureur de la République territorialement compétent sur les traitements, à la définition des personnes mises en cause, au principe de limitation de la durée de conservation des informations, au droit à l'effacement ou à la mise à jour dans certaines conditions, tant pour les personnes mises en cause que pour les victimes.

Cependant les fichiers de police judiciaire, comme tous les autres fichiers nominatifs, doivent respecter l'ensemble des conditions définies par la loi du 6 janvier 1978, notamment la consultation de la CNIL lors de la création de tout nouveau traitement, afin que soient précisément définies dans chaque cas la finalité du traitement, les catégories d'informations nominatives enregistrées, les infractions retenues, les modalités du droit d'accès ou la sécurité du traitement.

La Commission considère donc que référence explicite à la loi du 6 janvier 1978 devrait être faite dans l'article 9 du projet.

Elle estime en outre que la possibilité qui serait reconnue aux services de police et de gendarmerie d'enregistrer et de conserver, dans les fichiers de police judiciaire, des informations sur des personnes « sans limitation d'âge », pose le problème du signalement des enfants dans ces fichiers au regard des dispositions relatives à la responsabilité pénale des mineurs.

2) Le projet de loi ouvre la possibilité de consulter les fichiers de police judi ciaire, non seulement pour les besoins de certaines missions de police administrative ou de sécurité comportant des risques d'atteinte à l'ordre public ou à la sécurité des personnes, mais aussi pour la réalisation d'enquêtes et de tâches de vérification admi nistratives nombreuses et permanentes, pratiquées sur l'ensemble du territoire, telles que l'instruction des demandes d'acquisition de la nationalité française, celle des demandes de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers, ainsi que la nomination et la promotion dans les ordres nationaux.

Cette extension risque de faire jouer aux fichiers de police judiciaire le rôle d'un casier judiciaire parallèle moins contrôlé alors même que leur objet, leurs conditions d'accès, les modalités structurelles de leur alimentation et les délais inévitables

de toute mesure d'effacement ou de mise à jour doivent en faire seulement un instrument de police judiciaire, sauf dans quelques cas bien précis et rigoureusement contrôlés.

À cela s'ajoute le fait que la consultation à des fins administratives serait possible même lorsque la procédure judiciaire est en cours, c'est-à-dire avant que l'on sache si la personne mise en cause ne fera pas en définitive l'objet d'un acquittement, d'une mesure de relaxe, d'un non-lieu ou d'un classement sans suite, comme il s'en produit plus de 300 000 par an.

En tout état de cause, l'élargissement de l'accès à des informations sur les antécédents judiciaires des personnes visées par certaines enquêtes administratives de sécurité supposerait une réflexion complémentaire sur le rôle du casier judiciaire dans ce domaine.

La Commission appelle en conséquence l'attention sur les graves dangers d'atteinte aux libertés individuelles et au respect des droits des personnes susceptibles de résulter de l'utilisation des fichiers de police judiciaire pour des enquêtes ou d'autres tâches administratives.

Elle estime que la consultation des fichiers de police judiciaire ne peut intervenir qu'à des fins de « missions de police administrative ou de sécurité », et seulement dans des conditions précises, lorsque la nature de ces missions ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et selon des modalités rigoureuses d'habilitation des personnes pouvant y avoir accès, comme la Commission l'a déjà admis. Sur ce point, le décret prévu en application de l'article 9, qui sera pris après avis de la CNIL, précisera les conditions dans lesquelles les informations pourront être communiquées dans le cadre de « missions de police administrative ou de sécurité ».

La Commission estime qu'elle devrait également être consultée sur le décret fixant la liste des emplois et fonctions pour lesquels l'enquête administrative peut donner lieu à consultation des fichiers de police.

Sur le fichier national automatisé des empreintes génétiques

Le projet de loi modifie substantiellement le champ d'application du fichier national automatisé des empreintes génétiques tant en ce qui concerne les infractions visées que les personnes.

Le projet de loi étend ainsi le champ des infractions concernées, actuellement limité aux infractions sexuelles et à certains crimes, à de nombreux délits de violence contre les personnes et d'atteinte aux biens, ou mettant en danger l'ordre public, comme les délits en matière d'armes et d'explosifs.

Mais la modification principale introduite par le projet concerne les critères d'inscription dans le fichier. Pourront désormais y figurer les personnes *« à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis l'une des infractions visées à l'article 706-55 (du Code de procédure pénale) ».* Leurs empreintes génétiques pourront être conservées dans le fichier alors que jusqu'à présent seules l'étaient les empreintes génétiques des personnes condamnées.

Une telle extension modifie profondément la nature du fichier et appelle en conséquence des garanties nouvelles s'agissant tout particulièrement des modalités d'alimentation de ce fichier ainsi que des règles de conservation et d'effacement des informations.

— La Commission prend ainsi acte que le fichier national automatisé des empreintes génétiques demeure placé sous le contrôle d'un magistrat et relève avec satisfaction que les empreintes génétiques ne pourront être réalisées qu'à partir de segments d'ADN non codant, comme le précisent déjà les articles R. 53-9 et suivants du Code de procédure pénale, conformément aux souhaits qu'elle avait exprimé lors des avis favorables rendus sur les modalités de fonctionnement du fichier des empreintes génétiques.

La Commission observe que les empreintes génétiques des personnes soupçonnées pourront être conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction.

Elle estime que l'initiative de l'inscription dans ce fichier ne peut relever que des seuls magistrats précités et ne peut résulter de la seule décision d'un officier de police judiciaire, d'autant que le critère d'inscription des personnes suspectées — « une ou plusieurs raisons plausibles » — laisse une très grande marge d'appréciation ; qu'il doit en être de même en ce qui concerne les décisions de rapprochement de l'empreinte génétique d'une personne suspectée avec les données incluses dans le fichier.

— Au titre des garanties prévues, la Commission relève également que les empreintes ainsi conservées pourront être effacées sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, lorsque leur conservation n'apparaîtra plus nécessaire au regard de la finalité du fichier. Un double recours est prévu au bénéfice de l'intéressé dans le cas où le procureur n'a pas ordonné l'effacement, auprès du juge des libertés et de la détention puis, en cas de contestation de la décision de ce dernier, auprès du président de la chambre de l'instruction.

La Commission estime que des dispositions de suppression automatique des données devraient également être prévues lorsque la procédure est close et l'intéressé mis hors de cause, en particulier en cas de relaxe ou d'acquittement.

Elle prend bonne note qu'un décret en Conseil d'État, pris après avis de la CNIL, déterminera notamment la durée de conservation des informations enregistrées qui devra être fixée en fonction de l'âge et de la gravité de l'infraction.

À l'instar des dispositions prévues pour les fichiers de police judiciaire la loi devrait également préciser les destinataires des informations issues du fichier des empreintes génétiques.

Sur les autres dispositions

L'article 14 du projet de loi tend à autoriser l'installation de dispositifs fixes et permanents de contrôle des données signalétiques des véhicules afin de mieux lutter contre le vol de véhicules. La mise en œuvre de ces dispositifs devrait permettre de repérer les véhicules volés inscrits au fichier des véhicules volés.

La Commission estime que l'implantation de tels dispositifs ne doit pas porter atteinte au principe fondamental de la liberté d'aller et venir et que la durée de conservation des données de localisation doit être limitée au strict nécessaire.

Elle estime en conséquence qu'elle devrait être saisie pour avis du décret en Conseil d'Etat qui fixera les modalités d'application de cette disposition et en particulier la durée de conservation des données.

Poste et télécommunications

Délibération n° 02-014 du 14 mars 2002 portant avis sur un projet de décret relatif à l'annuaire universel et modifiant le Code des postes et télécommunications

La Commission nationale de l'informatique et des libertés ;

Saisie, par le secrétariat d'État à l'industrie, d'un projet de décret en Conseil d'Etat relatif à l'annuaire universel, modifiant le Code des postes et télécommunications ;

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

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

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

Vu la directive n° 98/10/CE du Parlement européen et du Conseil du 26 février 1998 concernant l'application de la fourniture d'un réseau ouvert (ONP) à la téléphonie vocale et l'établissement d'un service universel des télécommunications dans un environnement concurrentiel ;

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

Vu la loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications ;

Vu le Code des postes et télécommunications, notamment ses articles L. 33-4, L. 35-4 et D. 98-1 ;

Vu le décret n° 2002-36 du 8 janvier 2002 relatif à certaines clauses types des cahiers des charges annexés aux autorisations délivrées en application de l'article L. 33-1 du Code des postes et télécommunications ;

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

Vu le projet de décret présenté par le secrétariat d'État à l'industrie relatif à l'annuaire universel et modifiant le Code des postes et télécommunications ;

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

Formule les observations suivantes :

Le projet de décret consacre le droit pour tout abonné de figurer sur une liste d'abonnés ou d'utilisateurs, parallèlement au droit de s'opposer à être mentionné sur une telle liste. Il fait obligation à chaque opérateur de tenir la liste de ses abonnés et de la communiquer aux fins d'établissement d'un annuaire universel ou de mise en place d'un service de renseignements téléphoniques universel dans des conditions assurant la libre concurrence dans ces secteurs. Il prévoit par ailleurs que France Télécom doit éditer un annuaire universel sous formes imprimé et électronique et fournir un service universel de renseignements.

Le projet de décret comporte de nombreuses dispositions touchant à la protection des données personnelles des abonnés à la téléphonie fixe ou mobile.

Sur le sort des abonnés à la téléphonie mobile

L'article 4 du projet de décret, en ce qu'il s'applique notamment à la téléphonie mobile, impose aux opérateurs et à leurs distributeurs l'obligation d'informer leurs abonnés à la téléphonie mobile de leur droit à figurer dans les listes d'abonnés et des droits d'opposition qui en sont le pendant. Les abonnés concernés disposeraient d'un délai de six mois à compter de la réception de ladite information pour faire part de leur refus de figurer sur ces listes. À défaut, ils seraient réputés avoir consenti à y être mentionnés. Les utilisateurs des cartes prépayées ne figureraient, eux, sur les listes d'abonnés qu'à leur demande (dernier alinéa de l'article R. 10 nouveau).

Ce dispositif de consentement présumé, à l'expiration d'un délai de six mois, institue, en pratique, une procédure d'inscription obligatoire, sauf expression manifeste d'une opposition. La Commission l'estime en l'état insuffisante à garantir l'exercice éclairé de leurs droits par les 38 millions d'abonnés à la téléphonie mobile dont le numéro ne figure, à ce jour, dans aucun annuaire et qui ont coutume de n'être appelés que par des personnes auxquelles ils ont volontairement communiqué leur numéro.

Les conséquences pratiques pour les personnes inattentives ou peu conscientes de la portée de ce choix, ou qui n'auront pas réagi à temps méritent en effet d'être pesées : non seulement leur numéro de téléphone mobile figurera dans l'annuaire sans qu'elles en aient manifesté le souhait, mais y figurera aussi leur adresse complète puisque tel est le droit commun sauf opposition. De plus, dans l'hypothèse d'une négligence ou d'une inattention au document d'information qui devrait leur être adressé, les personnes concernées n'auront pas exercé, lors de l'inscription automatique de leur numéro de téléphone mobile dans un annuaire, leur droit de demander le bénéfice de l'inscription en liste orange, ce qui autoriserait tous les opérateurs de marketing à les solliciter téléphoniquement, ni de demander leur inscription en liste rouge.

De surcroît, le projet de décret prévoyant par ailleurs que l'exercice du droit à ne pas voir son numéro communiqué par un service de renseignement n'est pas gratuit, une telle procédure d'inscription automatique reviendrait à contraindre tous les abonnés à la téléphonie mobile à devoir s'acquitter d'une somme pour que leur numéro de téléphone ne soit pas divulgué.

Le projet de décret, sous le couvert de donner effet au droit nouveau des utilisateurs de téléphonie mobile de figurer dans un annuaire, institue un système d'inscription obligatoire sauf démarche explicite, spécifique et non-gratuite afin de demeurer dans le statut de protection complète dont bénéficient actuellement ces abonnés. De plus, il institue un régime différent, créant une rupture d'égalité de traitement, entre, d'une part, les abonnés dans le cadre d'un forfait et, d'autre part, les utilisateurs de téléphones mobiles usant du moyen des cartes prépayées qui, eux, continueraient, sauf demande expresse de figurer dans l'annuaire, de bénéficier de la protection qui existe actuellement.

Au total, dans la mesure où le droit pour tout abonné de s'opposer à figurer dans un annuaire est clairement reconnu par le texte présenté, la Commission estime, compte tenu de l'usage auquel 38 millions de personnes sont aujourd'hui accoutumées, qu'il serait plus conforme à l'esprit de protection des données personnelles et de la vie privée des personnes concernées de retenir un dispositif prévoyant que seules les personnes qui en auraient manifesté expressément la volonté puissent être ins-

crites dans un annuaire ou voir leur numéro de téléphone communiqué par un service de renseignements.

À défaut, le dispositif inverse prévu par le projet de décret ne pourrait être regardé comme assurant un authentique et complet exercice du droit d'opposition reconnu à l'abonné avec une force égale au droit de figurer dans l'annuaire que si la totalité de la protection souhaitée par l'abonné lui était offerte gratuitement : ceci signifie qu'il faudrait alors que, sur ce point particulier, soit garantie aux abonnés la gratuité pour l'accès tant à la liste chamois qu'à la liste rouge.

Sur le maintien du caractère payant de l'inscription en liste rouge

La Commission regrette vivement le choix auquel procède le projet de décret de distinguer d'un côté l'exercice, gratuit, du droit d'opposition à figurer dans un annuaire public (liste « chamois ») et le maintien du caractère payant pour étendre ce droit d'opposition à la communication des données personnelles par les services de renseignements téléphoniques (liste rouge). La Commission ne peut que rappeler sa position constante en faveur d'une gratuité totale de la liste rouge.

Au surplus, la Commission souligne le risque réel de confusion que peut entraîner dans l'esprit du public le nouveau mécanisme envisagé, qui pourrait donner à penser à un grand nombre de personnes que le refus, désormais gratuit, de figurer dans un annuaire s'étendrait, comme aujourd'hui, aux listes utilisées par les services de renseignements.

La Commission est donc conduite à demander qu'à l'énumération des droits d'opposition gratuits de l'article R. 10 du projet de décret soit ajouté un alinéa supplémentaire ainsi rédigé : « — de ne *pas figurer sur les listes d'abonnés accessibles par les services de renseignements ».*

À défaut, la Commission demande qu'une action de grande envergure soit réalisée et renouvelée à plusieurs reprises pour éclairer et informer de façon complète et très précise les abonnés sur leur choix.

Sur *l'utilisation des informations à des fins de prospection*

Le projet de décret, par son article R. 10-4 second alinéa, consacre une recommandation de la CNIL exprimée dans une délibération de 1997 qui permet aux personnes inscrites en liste « orange » d'être clairement identifiées dans tous les annuaires, quel que soit le support, par un signe distinctif. Il en résultera que toute utilisation des coordonnées des personnes inscrites en liste Orange à des fins de prospection commerciale par « *simple consultation »,* voire par téléchargement de l'annuaire, pourra désormais être clairement établie et sanctionnée. Les divers annuaires universels — nationaux ou départementaux — devront indiquer de manière visible l'opposition de l'abonné à l'utilisation des données qui le concernent dans le cadre d'opération de prospection. Il résulte de cette disposition un renforcement dès droits des personnes concernées.

Par ailleurs, le projet de décret punit de l'amende prévue pour les contraventions de la 5^{e} classe chaque prospection effectuée par télécopie ou par automates d'appels en infraction avec les dispositions des ordonnances de juillet et août 2001.

Ces deux séries de dispositions recueillent la pleine approbation de la Commission.

Catégories d'informations figurant sur les listes d'abonnés :

Les listes d'abonnés doivent comporter les informations suivantes : nom et/ou raison sociale ou dénomination sociale, prénoms, adresses et numéros de téléphone ainsi que la mention de la profession pour ceux qui le souhaitent. Une adresse

électronique peut être précisée à la demande de l'abonné, mais elle ne figurera que sur l'annuaire électronique.

Les abonnés à la téléphonie fixe pourront également demander l'insertion des données relatives aux autres utilisateurs de la ligne concernée, sous réserve de leur accord (article R. 10-4 alinéa 2).

Conformément aux prescriptions de la directive n° 97/*CE/66* du 15 décembre 1997 susvisée, il est prévu que l'abonné peut demander que son adresse ne figure pas dans son intégralité sur l'annuaire et qu'il ne soit pas fait référence à son sexe, ce qui signifie en pratique que le prénom pourra être limité à l'initiale.

Sur ce point, il y a lieu d'observer que le projet de décret supprime le dispositif antérieurement prévu par le décret relatif à certaines clauses types du cahier des charges des opérateurs de télécommunications qui subordonnait l'exercice de ces droits à la réserve que dans *« les données publiées ou communicables permettent de distinguer cette personne de* ses homonymes ». Cette précision devrait être maintenue et rappelée dans le projet.

De même, le décret ne prévoit pas de dispositif particulier dans le cas où un abonné exercerait, sciemment ou par inadvertance, les garanties qui lui sont offertes de manière différenciée selon les opérateurs dont il est le client.

Dans la mesure où chacun se voit reconnaître le droit de demander de faire figurer dans l'annuaire sa profession ou de ne pas mentionner son adresse complète ou de référence à son sexe et où l'annuaire dit « universel » comportera l'ensemble des lignes téléphoniques, fixes ou mobiles, d'une même personne, le décret pourrait être complété pour préciser la règle applicable en cas de divergences d'options choisies par un même abonné d'un opérateur à un autre de sorte que la responsabilité des éditeurs d'annuaire universel soit précisément définie.

L'accès à la liste universelle par certains services de l'État :

Le II de l'article 2 du projet de décret, par renvoi au f) de l'article D. 98-1 du Code des postes et télécommunications, prévoit que les services chargés de la sauvegarde de la vie humaine, des interventions de police, de la lutte contre l'incendie, de l'urgence sociale pourront, contre rémunération, obtenir communication des listes non expurgées des abonnés de chaque opérateur, c'est-à-dire, notamment, des personnes inscrites en liste rouge.

Si la Commission ne peut qu'être favorable à ce que les services d'urgence (SAMU, pompiers, police secours) puissent, dans le souci de la protection de la personne, disposer de moyens leur permettant d'identifier la personne appelante et son adresse, elle relève qu'en se bornant à imposer aux opérateurs l'obligation de communiquer leur liste d'abonnés sans préciser la finalité d'une telle communication et sans l'assortir de garanties particulières, le projet est de nature à faire naître le risque qu'au sein des organismes bénéficiaires puisse être reconstituée l'intégralité de la liste des abonnés en France, y compris les personnes inscrites en liste rouge, à d'autres fins que celle de l'identification de la personne appelante.

De la sorte, un très grand nombre de personnes, compte tenu de l'ensemble des services visés, pourrait disposer en permanence des informations relatives aux abonnés inscrits en liste rouge, portant ainsi atteinte à la confidentialité de ces informations.

En outre, l'expression de « services *publics chargés d'une intervention de police »* qui figure à l'article D. 98-1 apparaît susceptible de recouvrir d'autres services que les seuls services de police secours. Or, les services de police, autres que ser-

vices secours, ne peuvent aujourd'hui avoir accès aux informations inscrites en liste rouge que s'ils agissent en flagrant délit ou sur commission rogatoire d'un juge d'instruction, cas dans lesquels, compte tenu des prérogatives particulières qu'ils tiennent du Code de procédure pénale, leur est conférée la qualité de « tiers autorisé » au regard de la loi du 6 janvier 1978.

La Commission, sur ce point, prend acte de ce que le ministère en charge du projet a précisé que seuls les services de police secours, et non l'ensemble des services de police, devaient être bénéficiaires de cet accès.

Par ailleurs, si les services de l'urgence sociale peuvent légitimement bénéficier de la procédure des appels d'urgence (acheminement gratuit et prioritaire des appels), il y a lieu d'observer que la plupart d'entre eux s'engagent à respecter l'anonymat des appelants, élément de fait qui devrait conduire à exclure ces services du dispositif prévu d'accès à la liste universelle.

En définitive, la Commission estime que la rédaction du texte du projet de décret devrait être doublement modifié. D'une part, au lieu de procéder par renvoi à la liste des services publics figurant au f) de l'article D. 98-1 au Code des postes et télécommunications, le texte devrait énumérer directement et explicitement les seuls services publics bénéficiaires du dispositif, à savoir *« les services en charge de la sauvegarde de la vie humaine, de la lutte contre l'incendie et des interventions de police secours ».* D'autre part, le texte devrait être complété afin de préciser que la communication à ces services des listes non expurgées est justifiée « aux *fins exclusives d'identification de la personne appelante et de la connaissance de son adresse ».*

La détention et l'exploitation par les services publics visés ci-dessus des listes d'abonnés non expurgées nécessitera en tout état de cause, conformément à l'article 15 de loi du 6 janvier 1978, la présentation d'une demande d'avis auprès de la Commission nationale de l'informatique et des libertés, laquelle veillera aux conditions de mise en œuvre du dispositif technique et à ce que soient prévues toutes les mesures de sécurité destinées à protéger la confidentialité des informations ainsi conservées.

Sur les annuaires inversés

La Commission observe que le projet de décret n'évoque pas les « annuaires inversés » ou « services de renseignements inversés » qui permettent, à partir du seul numéro de téléphone, d'identifier le nom et l'adresse du titulaire de la ligne. La Commission a déjà eu l'occasion par le passé de souligner les risques particuliers que présente l'utilisation de tels outils permettant la collecte d'informations qu'une personne n'ayant laissé que son numéro de téléphone n'a pas entendu divulguer.

C'est à la suite de cette prise de position que France Télécom a, dans la pratique, pris en compte cette demande en créant la liste « Anti Qui-donc ». Compte tenu des dangers certains d'utilisation malveillante de tels annuaires, la Commission souhaite en encadrer leur utilisation par une généralisation et une consécration réglementaire de la pratique observée par France Télécom.

Elle demande donc que le projet de décret soit complété sur ce point en ajoutant à l'article R. 10 énumérant les droits d'opposition, un alinéa supplémentaire précisant : *« —* à ce *que les informations nominatives la concernant ne figurent pas dans des services de recherche inversée ou d'annuaire inversé accessible à tout public, l'exercice de ce droit n'étant pas opposable aux services publics énumérés au dernier alinéa du f) de l'article D. 98-1 du Code des postes et télécommunications. »*

Sur l'information des personnes

Si la diversité des listes d'opposition permet de mieux affiner le niveau de protection souhaitée, elle peut également être source d'équivoques des abonnés sur leurs droits. En outre, si la distinction entre la liste « chamois » et la liste rouge et la disparité des conditions d'exercice des droits reconnus aux personnes devaient subsister, il paraît particulièrement important que tous les abonnés soient clairement et précisément informés de leurs droits, des conditions d'exercice de ces droits ainsi que de leur portée. Aussi, la Commission estime-t-elle que devrait être ajouté un nouvel article R. 10-12 au projet de décret dans la rédaction suivante : *« L'opérateur est tenu d'informer individuellement chacun de ses abonnés, soit lors de la souscription ou de la modification du contrat, soit en cours d'exécution du contrat, des droits dont il dispose visés à l'article R. 10 ».*

Émet un avis favorable au projet présenté sous le bénéfice des observations et propositions de modifications de rédaction ci-dessus énoncées.

Délibération n° 02-071 du 15 octobre 2002 portant avis sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste relatif au fichier des nouveaux voisins

La Commission nationale de l'informatique et des libertés, saisie pour avis par La Poste, service national de l'adresse (SNA), d'un projet de décision du directeur général de La Poste portant création d'un traitement dénommé « fichier des nouveaux voisins » ;

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

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

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

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

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

Formule les observations suivantes :

La Poste (service national de l'adresse), a déposé une demande d'avis relative au « fichier des nouveaux voisins » dont la finalité principale est de permettre, d'une part, la collecte des changements d'adresse des particuliers ayant souscrit auprès de La Poste un contrat de réexpédition définitive, d'autre part, la commercialisation des changements d'adresse des personnes qui ne se sont pas opposées à une telle commercialisation aux sociétés liées contractuellement avec La Poste.

Les informations enregistrées dans le traitement sont relatives à l'identité du souscripteur du contrat (nom, prénom et sexe), l'identité des personnes membres du foyer du souscripteur (nom, prénom et sexe), l'ancienne adresse, la nouvelle adresse, l'ancien numéro de téléphone (facultatif), le nouveau numéro de téléphone (facultatif), la date de souscription du contrat de réexpédition définitif, la date de fin de validité du contrat de réexpédition définitif, l'accord de la personne pour la commercialisation de la nouvelle adresse.

Ces données sont recueillies directement auprès des personnes s'étant adressées à La Poste pour souscrire un contrat de réexpédition définitive du courrier, service proposé aux particuliers pour permettre le réacheminement de leur courrier pendant une durée d'une année après leur déménagement.

Les destinataires de ces informations sont les services de La Poste, les services des contributions directes ainsi que le régisseur du service de la redevance de l'audiovisuel en vertu de l'article L. 5 du Code des postes et des télécommunications s'agissant des seules informations les concernant, c'est-à-dire l'identité et la nouvelle adresse ; enfin, et dans la mesure où l'intéressé ne s'y est pas opposé, les organismes (banques, entreprises, commerces, associations, etc.) liés contractuellement à La Poste et qui ne détiennent pas obligatoirement l'ancienne adresse peuvent être destinataires de tout ou partie des données.

Les souscripteurs du contrat de réexpédition sont informés, sur le formulaire même de collecte des données, de la possibilité pour La Poste de communiquer les

données ainsi recueillies, non seulement, conformément aux obligations légales, au service des contributions directes et de la redevance de l'audiovisuel pour les seules coordonnées, mais aussi aux organismes (banques, entreprises, commerces, associations, etc.) liés contractuellement à La Poste, quels qu'ils soient.

Les intéressés sont mis en mesure de s'opposer à la communication aux organismes liés contractuellement à La Poste, au moyen d'une case à cocher, sur le formulaire de collecte des données, étant précisé que *« quelle que soit votre réponse, votre changement d'adresse sera traité dans les conditions habituelles. »*

Par ailleurs, il a été constaté que La Poste, sans attendre l'avis de la CNIL, procédait à une présentation, au demeurant inappropriée, de ce service tant dans une brochure publicitaire que sur le site internet du service national de l'adresse.

Prend acte que :

La Poste s'est engagée :

— à ne procéder à aucun « rapprochement » des fichiers de La Poste avec des fichiers appartenant à des sociétés tierces ;

— à apposer une nouvelle mention d'information sur les contrats de souscription plus explicite s'agissant de la nature des informations cédées et des destinataires des informations qui ne sont plus seulement les organismes qui étaient en possession de l'ancienne adresse des usagers mais tout organisme ;

— à modifier le site internet du service national de l'adresse et à renoncer à la diffu sion des plaquettes publicitaires faisant une présentation inappropriée du service des nouveaux voisins.

Emet un avis favorable au projet de décision présenté par le directeur général de La Poste sous les réserves suivantes :

1) Que La Poste s'engage à ne procéder à aucun « enrichissement » de ses fichiers avec des fichiers appartenant à des sociétés tierces.

2) Que la mention d'information sur le bordereau de souscription de change ment d'adresse définitif soit rédigée ainsi :

« La Poste souhaite commercialiser tout ou partie des informations collectées sur le formulaire en les cédant aux organismes qui en feraient la demande et qui ne détiennent pas forcément votre ancienne adresse (banques, entreprises, commerces, associations, etc.).

« En cas d'opposition à la cession aux organismes qui détenaient votre ancienne adresse cochez la case ci-contre.

« En cas d'opposition à la cession aux organismes qui ne détenaient pas votre ancienne adresse cochez la case ci contre.

« Quelle que soit votre réponse, votre changement d'adresse sera traité dans les conditions habituelles.

« Les indications recueillies ci-dessus donnent lieu à l'exercice d'un droit de rectification auprès du bureau de poste de votre choix ou auprès de votre centre opé*rationnel de l'adresse conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

« Dans tous les cas, La Poste est tenue de notifier les changements de domicile au service des contributions directes et au service de la redevance de l'audiovisuel conformément aux dispositions de l'article 92 de la loi n° 85-1407 du 30 décembre 1985 ».

3) Que les visas de la décision fassent référence aux différentes décisions prises précédemment par La Poste dans le cadre de la gestion des contrats de réexpé-

dition du courrier (décision de 1992 et décisions de 1998 relatives aux traitements Charade et Sérénade).

4) Que les articles 1 et 3 de la décision soient rédigés de la manière suivante :

Article 1 :

Il est créé à La Poste, service national de l'adresse, un traitement automatisé d'informations nominatives dont la finalité principale est la commercialisation des changements d'adresse des personnes qui ne se sont pas opposées à une telle commercialisation aux sociétés liées contractuellement.

Article 3 :

Les destinataires de ces informations sont :

— les services internes de La Poste à savoir la direction générale et les services comptables, les directions territoriales, le service national de l'adresse, les centres opérationnels de l'adresse et les bureaux de poste ;

— si l'intéressé ne s'y est pas opposé, les organismes (banques, entreprises, com merces, associations, etc.) liés contractuellement et qui ne détiennent pas obligatoire ment l'ancienne adresse, pour toutes les informations visées à l'article 2.

Prospection

Délibération n° 02-048 du 27 juin 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Saisie de plaintes et de demandes de renseignements relatifs à des opérations de prospection de masse par messages courts envoyés sur des téléphones mobiles (SMS) comportant le texte suivant « *Quelqu'un t'aime en secret et nous a chargé de te prévenir, devine qui a flashé sur toi en appelant le 08 ..... 1,35 €/appel + 0,34 €/min »,* ou un texte de même nature.

Au vu des plaintes et des demandes de renseignements téléphoniques, il apparaît que les envois massifs de ce type de SMS avaient pour principal objet de générer des appels sur un numéro audiotel sans qu'aucun tiers ne soit à l'origine du message initial, contrairement à ce qui était annoncé. En outre, lorsque les destinataires de ces appels ont rappelé le service audiotel pour savoir qui pouvait être à l'origine de ces messages, il leur a généralement été demandé de saisir les numéros de téléphone de ceux de leurs amis qu'ils estimaient pouvoir être à l'initiative d'un tel envoi. Ce faisant, les opérateurs enrichissaient leur base de données de prospection commerciale en y enregistrant de nouveaux numéros de téléphone.

L'effet de surprise jouant, un nombre considérable de personnes ont appelé ces services audiotel, élément confirmé par les services de la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes) qui évaluent à 3 millions le nombre de SMS envoyés pour le seul département des Hauts-de-Seine, appels qui ont généré, en retour, près de 180 000 appels vers les numéros audiotel indiqués.

La prospection massive par SMS résultant de l'utilisation d'un automate d'appel — défini comme « *un système automatisé d'appel sans intervention humaine »* selon les textes communautaires — il y a lieu, au préalable, de rappeler que, depuis une délibération n° 85-79 du 10 décembre 1985 portant réponse à une demande de conseil de la Direction générale des télécommunications sur l'utilisation des diffuseurs de messages pré-enregistrés par appels automatiques, la Commission considère que la diffusion de messages, opérée par automates d'appels pour le compte d'opérateurs public ou privé, est subordonnée à l'accord préalable et exprès, c'est-à-dire écrit, des intéressés.

Cette recommandation, dépourvue de force juridique mais néanmoins appliquée jusqu'alors par les différents acteurs du secteur, a trouvé sa consécration dans les ordonnances n° 2001-670 du 25 juillet 2001 transposant certaines dispositions de la directive n° 97/66/CE relative aux télécommunications et n° 2001-741

du 23 août 2001 transposant certaines dispositions de la directive n°97/7 relative à la vente à distance qui, respectivement, ont introduit dans le Code des postes et télécommunications un article L. 33-4-1 interdisant *« la prospection directe, par automates d'appels ou télécopieurs, d'un abonné ou d'un utilisateur d'un réseau de télécommunications qui n'a pas exprimé son consentement à recevoir de tels appels »* et, dans le Code de la consommation, un article L. 121-20-5 disposant *« Est interdite la prospection directe par un professionnel, au moyen d'automates d'appels ou de télécopieurs, d'un consommateur qui n'a pas exprimé son consentement à recevoir de tels appels ».*

Aussi, les pratiques relevées sont-elles contraires à ces dispositions.

En tout état de cause, et au regard de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'opération, prise dans son ensemble, paraît susceptible de tomber sous le coup des sanctions prévues aux articles 226-16 et 226-18 du Code pénal.

En effet, si les numéros de téléphone mobiles utilisés ont été, dans la plupart des cas, composés de manière automatique et aléatoire ou sont issus de fichiers de numéros achetés à des tiers, ces envois de SMS n'ont servi que d'accroché pour, non seulement générer des appels coûteux vers des services audiotel, mais aussi collecter auprès des personnes appelantes des numéros de téléphone commercialement utiles.

Or, le caractère licite et loyal d'une opération d'envoi de SMS ou de tout autre type de message par l'intermédiaire d'un tiers est subordonné d'une part, à ce que les titulaires des numéros de téléphone utilisés aient donné leur consentement préalable, d'autre part, à ce que les personnes destinataires des messages soient informées de l'identité de l'expéditeur.

De surcroît, en sollicitant des personnes ayant été contactées par SMS et appelant le service audiotel de leur communiquer les numéros de téléphone de leurs proches susceptibles selon elles, de se trouver à l'origine de l'envoi du message « texte » reçu, alors que ce message était un leurre, les sociétés en cause ont abusé de la crédulité de leurs correspondants et ont collecté les numéros de téléphone ainsi obtenus de manière déloyale et illicite.

Enfin, et en tout état de cause, la Commission relève que l'opération qui consiste, pour les entreprises commerciales concernées à constituer un fichier de numéros de téléphone portables, aurait dû être déclaré à la CNIL en application de l'article 16 de la 6 janvier 1978.

Or, sous réserve d'une identification précise des auteurs de ce type d'opération, aucun traitement d'informations nominatives de collecte de numéros de téléphone par de tels procédés n'a été déclaré à la Commission.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jette le discrédit sur les utilisations légales de ce type de prospection.

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :
— les opérations de collecte illicite et déloyale d'informations directement ou indirectement nominatives — en l'espèce les numéros de téléphone — à l'occasion d'un

démarchage par SMS, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;
— la mise en œuvre de traitements automatisés d'informations nominatives (en l'occurrence, la mise en oeuvre et la constitution de fichiers de numéros de téléphones mobiles à vocation commerciale) sans qu'il ait été procédé à la déclaration prévue par la loi, fait susceptible de constituer l'infraction visée à l'article 226-16 du Code pénal ;
— et **transmet au parquet** les éléments en sa possession susceptibles de lui per mettre l'identification des auteurs supposés des infractions tels qu'ils résultent de l'accomplissement par la CNIL de ses missions.

Délibération n° 02-054 du 9 juillet 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

Vu la directive n° 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 de données à caractère personnel et la libre circulation de ces données ;

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

Vu la délibération n° 02-043 du 23 mai 2002 de la Commission nationale de l'informatique et des libertés décidant une mission de contrôle d'un traitement automatisé d'informations directement ou indirectement nominatives mis en oeuvre ou utilisé à l'occasion de l'envoi d'un sondage politique sur internet ;

Vu le règlement intérieur de la Commission, et notamment son article *57* ;

Vu le rapport relatif à la mission de contrôle effectuée en application de la délibération n° 02-043 du 23 mai 2002, notifié aux sociétés Impact Net et Clara Net le 13 juin 2002 par courriers en recommandé avec accusé de réception ;

Vu les courriers d'observation adressés à la Commission par les sociétés Impact Net et Clara Net, respectivement les 26 et 27 juin 2002 ;

Après avoir entendu Madame Cécile Alvergnat, commissaire, en son rapport, et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement, en ses observations ;

Saisie par plusieurs internautes de la réception dans leur boîte aux lettres électronique, entre les deux tours des élections présidentielles, d'une enquête se présentant sous la forme d'un sondage politique intitulé « Le dernier sondage avant le second tour des élections présidentielles 2002 », réalisé par Sondage Express.

Cette enquête, sur laquelle apparaissaient deux logos, « Sondage express » et « 0K2Mail », comportait une première partie ayant pour objet de recueillir les intentions de vote des internautes au second tour des élections présidentielles, leur vote exprimé au premier tour, leur civilité, leur année de naissance et leur catégorie socio-professionnelle. Le mél adressé aux internautes indiquait « ce *sondage non nominatif est adressé à un panel de 100 000 internautes* » et comportait la mention suivante : *« Aucun fichier informatique nominatif n'est constitué par Sondage Express ».*

La deuxième partie du message était destinée à recueillir l'adresse électronique des personnes qui souhaitaient être informées des résultats ; les internautes ne souhaitant plus « participer aux sondages express » étaient de même invités à saisir leur adresse électronique. Aucune mention d'information relative aux prescriptions de l'article 27 de la loi du 6 janvier 1978 ne figurait sur le message, les internautes n'étant, en tout cas, pas informés que les données les concernant étaient susceptibles d'être communiquées à des tiers.

Le message comportait enfin une troisième partie permettant aux internautes de parrainer d'autres internautes en communiquant, par le biais d'un formulaire de collecte, dix adresses électroniques. Là encore, aucune mention d'information rela-

tive aux prescriptions de l'article 27 ne figurait sur le support de collecte des adresses électroniques des personnes dont l'adresse électronique était ainsi communiquée.

Les investigations menées par la Commission ont permis de constater que les deux logos figurant sur le mél adressé aux internautes correspondaient à deux noms de domaines enregistrés par la société Impact Net. Interrogée par les services de la Commission, la société Impact Net a reconnu qu'un fichier d'adresses électroniques établi dans le cadre de son site (101 cadeaux, corn), édité par ses soins, avait été utilisé pour adresser le sondage politique à 10 000 internautes mais précisait que l'opération était accomplie pour le compte d'un tiers. La Commission relevait que la déclaration de traitement automatisé d'informations nominatives relative au site 101 cadeaux effectuée en application de l'article 16 de la loi du 6 janvier 1978 par la société Impact Net précisait que les adresses électroniques collectées par ce site feraient exclusivement l'objet d'un usage interne et ne seraient pas communiquées ou utilisées pour le compte de sociétés extérieures.

Par délibération n° 02-043 en date du 23 mai 2002, la Commission a décidé de procéder à une mission de contrôle des traitements d'informations nominatives ayant permis l'envoi du sondage par internet, des traitements d'informations nominatives d'exploitation des adresses électroniques des internautes ayant répondu au sondage ou des personnes parrainées, ainsi que du traitement des résultats du sondage afin de s'assurer que ce dernier était dépourvu de tout caractère nominatif.

Cette mission de contrôle s'est déroulée le 5 juin 2002 auprès de la direction commerciale de la société Impact Net (61 rue Danton, 92000 Levallois-Perret) puis, le 6 juin 2002 auprès de la société Clara Net, hébergeur d'Impact Net, (68 rue du Faubourg St Honoré, 75008 Paris).

Les investigations menées par la délégation de la Commission le 5 juin 2002 auprès d'Impact Net ont permis d'identifier sur le serveur Cobalt de cette société, hébergé par Clara Net, un fichier-texte comportant 19 056 réponses au sondage politique associées, dans la auasi-totalité des cas (entre 12 000 et 13 000 réponses) aux adresses électroniques des internautes.

Étaient ainsi enregistrés dans ce traitement automatisé, en langage clair, l'adresse électronique de l'internaute, le nom du candidat pour lequel il avait déclaré avoir l'intention de voter au second tour des élections présidentielles, le caractère définitif ou non de cette intention, le nom du candidat pour lequel il avait voté au premier tour ou, le cas échéant, l'indication de son abstention, sa civilité, son année de naissance et sa catégorie socio-professionnelle.

1) Le gérant d'Impact Net, dans les observations qu'il a fait parvenir à la Commission par lettre recommandée avec accusé de réception en date du 26 juin 2002, conteste le *« caractère nominatif du fichier trouvé sur le serveur Cobalt »* au motif qu'il ne comporterait que des adresses électroniques et *« qu'à aucun moment les adresses e-mail associaient en même temps le nom, le prénom ou la société d'une personne ».*

Une telle analyse ne saurait emporter l'adhésion. En effet, de nombreuses adresses électroniques d'internautes ayant répondu au sondage comportent le nom de l'intéressé et l'initiale de son prénom, associés dans le fichier à d'autres renseignements (civilité, année de naissance, catégorie socio-professionnelle) ; en tout état de cause, ces adresses électroniques permettent à qui en dispose d'entrer en contact *via* internet avec ces correspondants et constituent des informations, directement ou indirectement, nominatives au sens de l'article 4 de la loi du 6 janvier 1978 qui précise que *« 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 ».

Dès lors, le fichier en cause constitue un traitement automatisé d'informations nominatives au sens de la loi du 6 janvier 1978.

Il résulte des constatations opérées par la Commission que la mention figurant dans le mél adressé aux internautes les informant que le sondage politique était non nominatif et qu'aucun traitement nominatif n'était constitué était mensongère, la collecte des informations nominatives ayant dès lors été opérée dans des conditions illicites et déloyales au sens de l'article 25 de la loi du 6 janvier 1978, infraction réprimée par l'article 226-18 du Code pénal.

En outre, le fichier des réponses au sondage, mis au jour par la mission de contrôle, comportant l'expression des opinions politiques des personnes concernées, il est contraire aux dispositions de l'article 31 de la loi du 6 janvier 1978 qui dispose qu'il est *« interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales, les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes ».*

Ainsi la mise en oeuvre et la conservation d'un tel fichier réalise l'infraction réprimée par l'article 226-19 du Code pénal.

2) Le gérant d'Impact Nef avance dans ses observations écrites qu'aucun élément ne permet d'établir que le fichier comportant les réponses au sondage poli tique associées aux adresses électroniques des internautes était placé sous sa respon sabilité. Il indique ainsi qu'Impact Net est étrangère à l'opération et qu'elle n'avait joué, en amont, que le rôle classique d'un loueur d'adresses, et, en aval, que le rôle de « sous-hébergeur » pour le compte d'autrui du fichier litigieux.

La Commission se bornera à observer, à ce stade, que le message adressé aux 100 000 internautes n'avait pour seul expéditeur que Sondage Express qui déclarait de surcroît explicitement le réaliser, que Sondage Express précisait ne constituer aucun fichier informatique nominatif, que les internautes ne souhaitant plus recevoir de message de ce type étaient invités à le faire savoir à Sondage Express, ce nom de domaine ayant été enregistré par la société Impact Net ; que le logo « OK2Mail » apparaissant dans le message est également un nom de domaine enregistré par Impact Net ; que le fichier litigieux a été retrouvé sur le serveur d'Impact Net, hébergé par Clara Net, sans qu'Impact Net ait produit quelque éventuel contrat de « sous-hébergément » au bénéfice d'un tiers ; qu'enfin, Impact Net a cru devoir supprimer purement et simplement ce fichier à l'issue des investigations de la Commission, initiative qui parait attester qu'elle en avait la responsabilité exclusive.

Il apparaît en outre vain de soutenir, comme le fait la société Impact Net, qu'elle n'aurait assuré qu'une prestation d'hébergement pour le compte d'un éventuel client et d'invoquer les dispositions de l'article 43-8 de la loi du 30 septembre 1986 relative à la liberté de communication, issues de la loi n° 2000-719 du 1er août 2000, qui exonère dans certaines conditions de toute responsabilité les personnes physiques ou morales qui assurent le stockage direct et permanent d'informations ou autres messages « pour mise à disposition du public ». En effet, il n'est pas contesté que le fichier mis au jour par la Commission n'avait ni pour nature ni pour vocation 'être mis à la disposition du public. Dès lors, les dispositions précitées ne sauraient être utilement invoquées par Impact Net pour échapper aux responsabilités qui sont les siennes.

4) Les investigations menées par la délégation de la Commission le 6 juin 2002 auprès de la société Clara Net, hébergeur de la société Impact Net, ont en

outre permis d'établir que des fichiers informatisés dans lesquels sont enregistrées des informations nominatives n'ont pas été déclarés par la société Impact Net à la Commission, en infraction avec l'article 16 de la loi du 6 janvier 1978 qui en fait obligation. Pour exemple, (lapme.net, courrierfinancier.com, courriermeaical.com) ou encore, (koobuycity.com) sont des noms de domaines de sites internet permettant la collecte de données personnelles qui ont été enregistrées dans le registre des noms de domaines — le « Whois ? » — par Impact Net.

Cette absence de déclarations de traitements automatisés d'informations nominatives auprès de la Commission, préalablement à leur mise en œuvre, constitue l'infraction réprimée par l'article 226-16 du Code pénal.

4) Enfin, Impact Net ne conteste pas avoir utilisé, dans le cadre de l'envoi du sondage en cause, un fichier d'adresses électroniques collectées à partir du site (101 cadeaux, corn) qu'elle édite mais fait valoir qu'une telle utilisation pour le compte de tiers serait régulière.

La Commission relève que si les mentions d'informations à destination des internautes qui se connectent sur ce site sont, au jour de la présente délibération, régulières au regard des exigences de la loi du 6 janvier 1978, le site (101 cadeaux, corn) était inaccessible au moment des investigations de la Commission et que la déclaration qui en a été faite à la CNIL le 16 juillet 2001, et non modifiée depuis lors, précise que les adresses électroniques collectées par ce site ne sont pas cédées à des tiers. Dès lors, l'utilisation qui a été faite des adresses électroniques collectées à partir de (101 cadeaux, com) n'est pas conforme à la déclaration faite à la CNIL en application de l'article 16 de la loi du 6 janvier 1978, ce qui constitue l'infraction prévue par l'article 226-16 du Code pénal.

L'ensemble de ces faits, susceptibles d'être imputables à la société en commandite simple Impact Net, et à tous autres, paraissent, à ce stade, suffisamment établis et constituent une atteinte caractérisée aux dispositions dont la CNIL a pour mission d'assurer l'application.

En revanche, il y a lieu d'observer que Clara Net, hébergeur d'Impact Net, est hors de cause.

En conséquence :

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

— la collecte d'adresses électroniques opérée par un moyen frauduleux, déloyal ou illicite en ce que les internautes sollicités ont été faussement informés que le sondage ne revêtait aucun caractère nominatif alors que leurs réponses étaient associées à leur adresse électronique, information indirectement nominative au sens de l'article 4 de la loi du 6 janvier 1978, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;

— la mise en œuvre d'un traitement automatisé d'informations nominatives faisant apparaître les opinions politiques des personnes, sans que leur consentement exprès ait été préalablement recueilli, en l'espèce, la collecte et l'enregistrement des votes exprimés au premier tour des élections présidentielles et des intentions de vote au second tour associés aux adresses électroniques des internautes et aux autres informations suivantes : année de naissance, civilité, catégorie socio-professionnelle, fait susceptible de constituer l'infraction visée par l'article 226-19 du Code pénal ;

— le fait de procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi du 6 janvier 1978, en l'espèce les informations nominatives collectées à partir des sites suivants : (lapme.net, courrierfinancier.com, courriermedical.com, koobuy-

city.com), faits susceptibles de constituer l'infraction visée par l'article 226-16 du Code pénal ;
— le fait d'avoir utilisé les adresses électroniques collectées à partir du site 101 cadeaux, com alors que la déclaration de traitement de ce site effectuée le 16 juillet 2001 et enregistrée sous le n° 761 393 DO précisait que les données ainsi collectées ne seraient pas utilisées pour le compte de tiers, fait susceptible de constituer l'infraction visée par l'article 226-16 du Code pénal.

Transmet au parquet la présente délibération accompagnée de la copie informatique du fichier litigieux.

Délibération n° 02-065 du 24 septembre 2002 portant avertissement à la société « Audit et solutions »

La Commission nationale de l'informatique et des libertés ;

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

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

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

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

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

Saisie d'une plainte concernant l'utilisation à des fins de prospection commerciale par la société Audit et Solutions d'un fichier regroupant des données concernant d'anciens élèves de grandes écoles ;

Formule les observations suivantes :

L'instruction de cette saisine fait apparaître que la société Audit et Solutions ne dispose pas d'un accord avec l'ensemble des associations d'anciens élèves dont les annuaires sont exploités.

Il n'appartient pas à la Commission de régler les litiges concernant les conditions commerciales d'utilisation de bases de données mais d'assurer la correcte application des dispositions de la loi du 6 janvier 1978 lorsque ces données présentent un caractère nominatif.

La Commission relève que les opérations décrites ci-dessus en ce qu'elles conduisent la société Audit et Solutions à collecter des informations nominatives sans s'assurer que les personnes concernées ne se sont pas opposées à un tel transfert d'informations relèvent de l'article 25 de la loi précitée qui interdit toute collecte déloyale ou illicite.

L'attention de la société Audit et Solutions a été appelée lors de l'instruction de la saisine sur le caractère déloyal et illicite de cette collecte. À ce jour, la société Audit et Solutions n'a toujours pas répondu aux différents courriers qui lui ont été adressés.

La Commission souligne que, conformément à l'article 21 de la loi du 6 janvier 1978, elle doit obtenir, dans les meilleurs délais, tous les renseignements utiles à l'exécution de sa mission afin que soient respectées les dispositions de la loi « informatique et libertés ».

En conséquence :

— **demande** à la société Audit et Solutions de se mettre en conformité avec les dispositions de la loi du 6 janvier 1978, notamment son article 25 ;

— **demande** d'être tenue informée des dispositions prises à cet effet ;

— **et décide,** faisant application des dispositions de l'article 21-4 de la loi n° 78-17 du 6 janvier 1978 **d'adresser un avertissement** à la société Audit et Solutions.

Délibération n° 02-074 *du* 24 octobre 2002 portant adoption du rapport relatif à l'opération « Boîte à spam »

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement réservée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

Cette initiative atteste de la volonté de la Commission d'appréhender le phénomène du *spamming* et d'apporter aux internautes qui en sont victimes des éléments, tant juridiques que techniques, leur permettant d'y faire face.

En conséquence, **décide** :

— d'adopter le rapport relatif à l'opération « boîte à spams » annexé à la présente délibération ;

— d'adresser ce rapport aux organismes et associations représentatifs des acteurs concernés par le publipostage électronique ;

— de faire une communication sur l'opération menée lors de la prochaine réunion du groupe de travail international sur la protection des données dans le secteur des télécommunications, dit « groupe de Berlin » ;

— de publier ce rapport sur le site internet de la CNIL.

Délibération n° 02-075 du 24 octobre 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

Vu la directive n° 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 de données à caractère personnel et la libre circulation de ces données ;

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement dédiée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

La Commission a, dans son rapport précité, défini la pratique du *spamming* comme étant : *« l'envoi massif— et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*

Le développement de ce type d'opérations trouve sa source dans les caractéristiques propres au réseau internet : en effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jettent le discrédit sur les utilisations légales de ce type de prospection.

De plus, les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».* Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Depuis l'ouverture de la boîte à lettre électronique spam@cnil.fr, le 10 juillet dernier, la Commission a reçu environ 650 messages d'internautes transférant un courrier électronique émanant de la société Alliance Bureautique Service. Les courriers électroniques reçus par les internautes comportaient un message commercial provenant de cette société alors que les intéressés indiquent n'avoir jamais été en contact avec cette dernière.

Les conditions dans lesquelles cette opération de prospection est effectuée sont manifestement contraires aux dispositions de la loi « informatique et libertés ».

Il s'avère, d'une part, que la société Alliance Bureautique Service utilise, afin de collecter les adresses électroniques des personnes qu'elle prospecte, un outil appelé « robot-mail » que cette société propose elle-même à la vente. L'utilisation d'un tel outil qui permet de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects est en totale opposition avec l'article 25 de la loi « informatique et libertés » qui énonce : « *La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

D'autre part, certaines des personnes démarchées ont indiqué qu'elles n'avaient pu exercer de manière effective le droit d'opposition qu'elles tiennent de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive CE n° 95/46 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.

Il ne leur a pas été possible de s'opposer à la réception de nouveaux messages en provenance de cette même société dans la mesure où le lien de désinscription n'a pas fonctionné.

Ces pratiques relèvent ainsi, et à double titre, de l'article 226-18 du Code pénal qui prévoit : *« Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

Enfin, et en tout état de cause, la Commission observe que l'opération qui consiste, pour une entreprise à constituer un fichier d'adresses électroniques à des fins de prospection commerciale, aurait dû être déclarée, avant sa mise en œuvre, à la CNIL en application de l'article 16 de la loi du 6 janvier 1978.

Or, la société Alliance Bureautique Service n'a pas, préalablement à la mise en œuvre du traitement automatisé d'informations nominatives lui servant de support à son opération de prospection, satisfait aux obligations de déclaration auprès de la Commission.

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :

— l'opération de collecte illicite et déloyale d'informations directement ou indirecte ment nominatives — en l'espèce les adresses électroniques des personnes démarchées

— et la mise en oeuvre de traitements automatisés d'informations nominatives malgré l'opposition, fondée sur des raisons légitimes, des personnes titulaires desdites adres ses, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;

— la mise en œuvre de traitements automatisés d'informations nominatives — en l'occurrence, la mise en œuvre et la constitution de fichiers d'adresses électroniques à des fins de prospection commerciale — sans qu'il ait été procédé à la déclaration préalable prévue par la loi, fait susceptible de constituer l'infraction visée à l'article 226-16 du Code pénal ;

— **et transmet au parquet** la présente délibération accompagnée de certains des messages transmis par les internautes et plaintes mettant en cause la société Alliance Bureautique Service.

Délibération n° 02-076 du 24 octobre 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement dédiée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

La Commission a, dans son rapport précité, défini la pratique du *spamming* comme étant : « *l'envoi massif— et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*

Le développement de ce type d'opérations trouve sa source dans les caractéristiques propres au réseau internet : en effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jettent le discrédit sur les utilisations légales de ce type de prospection.

De plus, les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* ». Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Depuis l'ouverture de la boîte à lettre électronique spam@cnil.fr, le 10 juillet dernier, la Commission a reçu environ 260 messages d'internautes transférant un courrier électronique faisant la promotion d'un site et de services minitel de rencontre. Après analyse des différents messages, il apparaît que ceux-ci émanent de la société BV Communication. Les internautes qui ont été destinataires de ces messages

ont, pour certains d'entre eux, précisé qu'ils n'avaient jamais été en contact avec cette dernière ni avec aucun des services qu'elle propose.

Les conditions dans lesquelles cette opération de prospection est effectuée sont manifestement contraires aux dispositions de la loi « Informatique et libertés ».

Il s'avère, d'une part, que la diversité des personnes démarchées et le fait que leurs adresses électroniques correspondent à un usage autant privé que professionnel donnent à penser que la collecte des données personnelles de ces personnes a été opérée à l'aide de « robots aspirateurs ». L'utilisation de tels outils qui permettent de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects est en totale opposition avec l'article 25 de la loi « informatique et libertés » qui énonce : « *La collecte* de *données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

D'autre part, certaines des personnes démarchées ont indiqué qu'il ne leur était pas possible d'exercer de manière effective le droit d'opposition qu'elles détiennent de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive CE n° 95/46 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.

Il ne leur a pas été possible de s'opposer, à l'avenir, à la réception de nouveaux messages en provenance de cette même société.

Ces pratiques relèvent ainsi, et à double titre, de l'article 226-18 du Code pénal qui prévoit : « *Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

Enfin, et en tout état de cause, la Commission observe que l'opération qui consiste, pour une entreprise à constituer un fichier d'adresses électroniques à des fins de prospection commerciale, aurait dû être déclarée à la CNIL en application de l'article 16 de la loi du 6 janvier 1978.

Or, aucun traitement d'informations nominatives émanant de la société BV Communication n'a été, à ce jour, déclaré à la Commission.

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :
— l'opération de collecte illicite et déloyale d'informations directement ou indirecte ment nominatives — en l'espèce les adresses électroniques des personnes démarchées
— et la mise en œuvre de traitements automatisés d'informations nominatives malgré l'opposition, fondée sur des raisons légitimes, des personnes titulaires desdites adres ses, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;
— la mise en œuvre de traitements automatisés d'informations nominatives — en l'occurrence, la mise en œuvre et la constitution de fichiers d'adresses électroniques à des fins de prospection commerciale — sans qu'il ait été procédé à la déclaration prévue par la loi, fait susceptible de constituer l'infraction visée à l'article 226-16 du Code pénal ;
— et **transmet au parquet** la présente délibération accompagnée de certains des messages transmis par les internautes mettant en cause la société BV Communication.

Délibération n° 02-077 du 24 octobre 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement dédiée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

La Commission a, dans son rapport précité, défini la pratique du *spamming* comme étant : « *l'envoi massif— et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*

Le développement de ce type d'opérations trouve sa source dans les caractéristiques propres au réseau internet : en effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jettent le discrédit sur les utilisations légales de ce type de prospection.

De plus, les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».* Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Depuis l'ouverture de la boîte à lettre électronique spam@cnil.fr, le 10 juillet dernier, la Commission a reçu environ 500 messages d'internautes transférant un courrier électronique émanant de la société GREAT-MEDS.COM. Les courriers électroniques reçus par les internautes comportaient un message commercial provenant de cette société alors qu'ils n'avaient jamais été en contact avec cette dernière. Ces

messages comportaient différents textes et liens qui, tous, permettaient à l'internaute démarché de se rendre sur le site (great-meds. corn). Cette société propose, à la vente, divers produits à vocation pharmaceutique. Il apparaît ainsi qu'une seule et même société, située sur le territoire des États-Unis, se trouve à l'origine de ces opérations de prospection.

Les conditions dans lesquelles cette opération de prospection est effectuée sont manifestement contraires aux dispositions de la loi « informatique et libertés ».

Il s'avère, d'une part, que la diversité des personnes démarchées et le fait que leurs adresses électroniques correspondent à un usage autant privé que professionnel donnent à penser que la collecte des données personnelles de ces personnes a été opérée à l'aide de 'robots aspirateurs'. L'utilisation de tels outils qui permettent de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects est en totale opposition avec l'article 25 de la loi « informatique et libertés » qui énonce : *« La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

D'autre part, certaines des personnes démarchées ont indiqué qu'il ne leur était pas possible d'exercer de manière effective le droit d'opposition qu'elles détiennent de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive CE n° 95/46 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. La procédure de désinscription indiquée dans les messages n'est, en effet, pas effective.

Ainsi, il n'a pas été possible aux personnes démarchées de s'opposer, à l'avenir, à la réception de nouveaux messages en provenance de cette même société, leurs données personnelles continuant d'être utilisées malgré leur opposition.

Ces pratiques relèvent ainsi, et à double titre, de l'article 226-18 du Code pénal qui prévoit : « *Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978 et de l'article 113-7 du Code pénal qui énonce : *« La loi pénale française est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de l'infraction »,* de dénoncer au parquet :
— l'opération de collecte illicite et déloyale d'informations directement ou indirecte ment nominatives — en l'espèce les adresses électroniques des personnes démar chées — et la mise en oeuvre de traitements automatisés d'informations nominatives malgré l'opposition, fondée sur des raisons légitimes, des personnes titulaires desdi tes adresses, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;
— **et transmet au parquet** la présente délibération accompagnée de certains des messages transmis par les internautes et des informations qui en sont issues met tant en cause la société GREAT-MEDS-COM.

Délibération n° 02-078 du 24 octobre 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement dédiée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

La Commission a, dans son rapport précité, défini la pratique du *spamming* comme étant : « *l'envoi massif— et parfois répété —* de *courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*

Le développement de ce type d'opérations trouve sa source dans les caractéristiques propres au réseau internet : en effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jettent le discrédit sur les utilisations légales de ce type de prospection.

De plus, les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».* Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Depuis l'ouverture de la boîte à lettre électronique spam@cnil.fr, le 10 juillet dernier, la Commission a reçu environ 170 messages d'internautes transférant un courrier électronique émanant de la société SUNILES. Les courriers électroniques reçus par les internautes comportaient un message commercial provenant de cette société alors qu'ils n'avaient jamais été en contact avec cette dernière.

Les conditions dans lesquelles cette opération de prospection est effectuée sont manifestement contraires aux dispositions de la loi « Informatique et libertés ».

Il s'avère, d'une part, que la diversité des personnes démarchées et le fait que leurs adresses électroniques correspondent à un usage autant privé que professionnel donnent à penser que la collecte des données personnelles de ces personnes a été opérée à l'aide de « robots aspirateurs ». L'utilisation de tels outils qui permettent de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects est en totale opposition avec l'article 25 de la loi « informatique et libertés » qui énonce : *« La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

D'autre part, certaines des personnes démarchées ont indiqué qu'il ne leur était pas possible d'exercer de manière effective le droit d'opposition qu'elles détiennent de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive CE n° 95/46 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.

Il ne leur a pas été possible de s'opposer, à l'avenir, à la réception de nouveaux messages en provenance de cette même société dans la mesure où le lien de désinscription n'a pas fonctionné.

Ces pratiques relèvent ainsi, et à double titre, de l'article 226-18 du Code pénal qui prévoit : *« Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

Enfin, et en tout état de cause, la Commission observe que l'opération qui consiste, pour une entreprise à constituer un fichier d'adresses électroniques à des fins de prospection commerciale, aurait dû être déclarée à la CNIL en application de l'article 16 de la loi du 6 janvier 1978.

Or, aucun traitement d'informations nominatives émanant de la société SUNILES n'a été, à ce jour, déclaré à la Commission.

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :

— l'opération de collecte illicite et déloyale d'informations directement ou indirecte ment nominatives — en l'espèce les adresses électroniques des personnes démar chées — et la mise en oeuvre de traitements automatisés d'informations nominatives malgré l'opposition, fondée sur des raisons légitimes, des personnes titulaires desdi tes adresses, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;

— la mise en œuvre de traitements automatisés d'informations nominatives — en l'occurrence, la mise en œuvre et la constitution de fichiers d'adresses électroniques à des fins de prospection commerciale — sans qu'il ait été procédé à la déclaration prévue par la loi, fait susceptible de constituer l'infraction visée à l'article 226-16 du Code pénal ;

— **et transmet au parquet** la présente délibération accompagnée de certains des messages transmis par les internautes mettant en cause la société SUNILES.

Délibération n° 02-079 du 24 octobre 2002 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

La Commission nationale de l'informatique et des libertés ;

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

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

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

Après avoir entendu Madame Cécile Alvergnat en son rapport et Madame Charlotte-Marie Pitrat, commissaire du Gouvernement en ses observations ;

Dans la continuité de son rapport sur *Le publipostage électronique et la protection des données personnelles,* adopté en séance plénière le 14 octobre 1999, la Commission nationale de l'informatique et des libertés a décidé, en juillet 2002, d'ouvrir une boîte à lettres électronique spam@cnil.fr spécialement dédiée à la réception de courriers électroniques non sollicités, plus couramment appelés *spams,* que les internautes auraient reçus et qu'ils y auraient transférés.

La Commission a, dans son rapport précité, défini la pratique du *spamming* comme étant : *« l'envoi massif— et parfois répété — de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*

Le développement de ce type d'opérations trouve sa source dans les caractéristiques propres au réseau internet : en effet, à la différence des autres types de prospection, la captation des coordonnées personnelles y est aisée, en même temps que le coût final de la prospection est principalement supporté par les personnes démarchées en ce que la réception de tels messages augmente le temps de connexion au réseau.

La Commission ne peut que relever le caractère néfaste de telles opérations qui portent atteinte à la tranquillité des personnes démarchées et jettent le discrédit sur les utilisations légales de ce type de prospection.

De plus, les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : « Sont réputées nominatives au sens *de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».* Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom.

Depuis l'ouverture de la boîte à lettre électronique spam@cnil.fr, le 10 juillet dernier, la Commission a reçu environ un millier de messages d'internautes transférant un courrier électronique faisant la promotion de sites pornographiques sous la forme d'une lettre *Le Top 50 des sites X.* Les internautes qui ont été destinataires de ces messages ont, pour certains d'entre eux, précisé qu'ils n'avaient jamais été en contact avec un ou plusieurs sites de cette nature.

Les conditions dans lesquelles cette opération de prospection est effectuée sont manifestement contraires aux dispositions de la loi « Informatique et libertés ».

Il s'avère, d'une part, que la diversité des personnes démarchées et le fait que leurs adresses électroniques correspondent à un usage autant privé que professionnel donnent à penser que la collecte des données personnelles de ces personnes a été opérée à l'aide de « robots aspirateurs ». L'utilisation de tels outils qui permettent de collecter des adresses électroniques figurant dans les espaces publics de l'internet (forums de discussion, pages personnelles ou d'entreprises, etc.) et de se constituer ainsi, à moindre coût, des fichiers de prospects est en totale opposition avec l'article 25 de la loi « Informatique et libertés » qui énonce : *« La collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdite ».*

D'autre part, certaines des personnes démarchées ont indiqué qu'il ne leur était pas possible d'exercer de manière effective le droit d'opposition qu'elles détiennent de l'article 26 de la loi du 6 janvier 1978 et de l'article 14 de la directive CE n° 95/46 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.

Il ne leur a pas été possible de s'opposer, à l'avenir, à la réception de nouveaux messages en provenance de cette même société.

Ces pratiques relèvent ainsi, et à double titre, de l'article 226-18 du Code pénal qui prévoit : *« Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives malgré l'opposition de la personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».*

Enfin, et en tout état de cause, la Commission observe que l'opération qui consiste, pour une entreprise à constituer un fichier d'adresses électroniques à des fins de prospection commerciale, aurait dû être déclarée à la CNIL en application de l'article 16 de la loi du 6 janvier 1978.

Or, sous réserve d'une identification précise des auteurs de cette opération, aucun traitement d'informations nominatives de prospection en faveur de sites pornographiques n'a été, à ce jour, déclaré à la Commission.

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

En conséquence :

Décide, en application des dispositions de l'article 21-4° de la loi du 6 janvier 1978, de dénoncer au parquet :

— l'opération de collecte illicite et déloyale d'informations directement ou indirecte ment nominatives — en l'espèce les adresses électroniques des personnes démarchées

— et la mise en œuvre de traitements automatisés d'informations nominatives malgré l'opposition, fondée sur des raisons légitimes, des personnes titulaires desdites adres ses, fait susceptible de constituer l'infraction visée par l'article 226-18 du Code pénal ;

— la mise en œuvre de traitements automatisés d'informations nominatives — en l'occur rence, la mise en œuvre et la constitution de fichiers d'adresses électroniques à des fins de prospection commerciale — sans qu'il ait été procédé à la déclaration prévue par la loi, fait susceptible de constituer l'infraction visée à l'article 226-16 du Code pénal ;

— et **transmet au parquet** la présente délibération ainsi que les éléments en sa possession, à savoir certains des messages transmis par les internautes et les informa tions qui en sont issues, susceptibles de lui permettre l'identification des auteurs suppo sés des infractions tels qu'ils résultent de l'accomplissement par la CNIL de sa mission.

Santé

Délibération n° 02-003 du 5 février 2002 portant avis sur un projet de décret fixant les modalités de la transmission de données individuelles prévues à l'article L. 3622-6 du Code de la santé publique et les garanties du respect de l'anonymat des personnes qui s'y attachent

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le directeur des sports du ministère de la Jeunesse et des Sports d'un projet de décret fixant les modalités de la transmission de données individuelles prévues à l'article L. 3622-6 du Code de la santé publique et les garanties de l'anonymat des personnes qui s'y attachent ;

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

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

Vu le Code de la santé publique ;

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

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

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

Formule les observations suivantes :

Le ministère de la Jeunesse et des Sports a saisi la Commission, pour avis, d'un projet de décret prévu en application des dispositions de l'article L. 3622-7 du Code de la santé publique issues de la loi du 23 mars 1999 relative à la protection de la santé des sportifs et à la lutte contre le dopage, qui a notamment pour objet de prévoir les modalités de transmission aux autorités sanitaires de données individuelles recueillies par les médecins qui traitent des cas de dopage ou de pathologies consécutives à des pratiques de dopage ainsi que les garanties du respect de l'anonymat des personnes.

Les modalités de la surveillance médicale des sportifs prévues par la loi du 23 mars 1999 précitée imposent à tout médecin qui décèle chez un sportif des signes évoquant une pratique de dopage, de refuser la délivrance de certificats médicaux, d'informer son patient des risques encourus du fait de cette pratique et du suivi médical dont il peut bénéficier, de transmettre obligatoirement au médecin responsable d'une antenne médicale spécialisée dans le dopage, sous forme nominative, les constatations faites et d'en informer son patient.

Cette surveillance médicale s'accompagne également d'un dispositif de recueil et de transmission à des fins épidémiologiques de données individuelles qui permettra d'évaluer l'état du dopage en France et d'orienter plus efficacement les politiques de santé et d'éducation.

Le projet de décret a pour objet de décrire les modalités de la transmission des informations individuelles et les mesures retenues pour garantir l'anonymat des personnes concernées en reprenant un dispositif analogue à celui défini par les pouvoirs publics pour fixer les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire sur lequel la Commission s'est prononcée par une délibération n° 00-045 du 3 octobre 2000.

Sur l'obligation de transmission

Elle est définie à l'article premier du projet de décret qui, reprenant les termes de l'article L. 3622-6 du Code de la santé publique, dispose que *« les médecins qui traitent des cas de dopage ou de pathologies consécutives à une pratique de dopage sont tenus de transmettre, sous forme anonyme, les données individuelles relatives à ces cas à la cellule scientifique du Conseil de prévention et de lutte contre le dopage, contribuant ainsi à la veille sanitaire par un recueil de données à des fins épidémiologiques ».*

La cellule scientifique de coordination de la recherche fondamentale et appliquée dans les domaines de la médecine sportive et du dopage, composée en particulier de personnes spécialisées en toxicologie et pharmacologie est placée auprès du conseil de prévention et de lutte contre le dopage, autorité administrative indépendante. Elle sera destinataire des données individuelles par l'intermédiaire des médecins responsables des antennes médicales de lutte contre le dopage qui, implantées dans des établissements publics de santé, sont placées sous la responsabilité d'un médecin ayant une pratique en pharmacologie, toxicologie ou dans la prise en charge des dépendances.

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

Sur les garanties d'anonymat

L'article quatre du projet de décret prévoit qu'une fiche de déclaration sera établie par le médecin responsable de l'antenne médicale de lutte contre le dopage à partir des informations transmises par le médecin traitant. Elle comportera les coordonnées de l'antenne médicale et de son médecin responsable, les coordonnées du médecin traitant et notamment son nom, son prénom et son adresse, les coordonnées d'un autre prescripteur ou d'une tierce personne à l'origine de l'orientation de la personne vers l'antenne médicale. Elle comportera également un numéro d'anonymat établi par codage informatique irréversible à partir des trois premières lettres du nom, du prénom et de la date de naissance et du sexe de la personne.

Il est également prévu que « *le médecin responsable de l'antenne médicale de lutte contre le dopage qui établit la correspondance entre le numéro d'anonymat et les éléments d'identité de la personne en assure la conservation, aux fins de validation et d'exercice du droit d'accès, dans des conditions garantissant la confidentialité des informations et la détruit six mois après la date d'envoi des données à la cellule scientifique du conseil de prévention et de lutte contre le dopage. »*

La Commission constate avec satisfaction que le projet de décret prévoit la mise en place, à l'égal du dispositif retenu pour la notification des maladies à déclaration obligatoire, un dispositif d'anonymisation à la source des éléments d'identification de Ta personne par technique de codage irréversible qui est de nature à concilier tout à la fois la nécessité pour la recherche épidémiologique de disposer de données fiables tout en garantissant l'anonymat de la personne.

La Commission relève qu'aux termes du dernier alinéa de l'article quatre du projet de décret : *« Un arrêté conjoint des ministres chargés des Sports et de la Santé, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les*

données, notamment socio-démographiques, sportives, cliniques, biologiques, pharmacologiques et thérapeutiques que le médecin de l'antenne médicale de lutte contre le dopage reporte sur la fiche mentionnée au présent article ».

Sur les modalités de transmission des informations

L'article trois du projet de décret prévoit que le médecin traitant ayant constaté un cas de dopage ou une pathologie consécutive à un cas de dopage transmettra au médecin responsable de l'antenne médicale de lutte contre le dopage, soit par voie postale sous pli confidentiel portant la mention secret médical, soit par télétransmission après chiffrement des données, les trois premières lettres du nom, du prénom ainsi que la date de naissance et le sexe de la personne. Il transmettra également les éléments utiles à la rédaction de la fiche qui sera établie par le médecin responsable de l'antenne médicale.

Le médecin responsable de l'antenne médicale de lutte contre le dopage transmettra alors la fiche qu'il aura établie accompagnée du numéro d'anonymat établi par codage informatique soit par voie postale sous pli confidentiel portant la mention secret médical, soit par télétransmission après chiffrement des données au médecin responsable de la cellule scientifique du conseil de prévention et de lutte contre le dopage qui, selon les mêmes modalités, les transmettra à l'Institut de veille sanitaire chargé, conformément aux dispositions de l'article L. 1413-2 du Code de la santé publique de l'observation permanente de l'état de santé de la population.

La Commission relève également qu'aux termes de l'article sept du projet de décret les personnes appelées à connaître, à quelque titre que ce soit, des données individuelles ainsi transmises, seront astreintes au secret professionnel tel qu'il est défini par l'article 226-13 du Code pénal.

Ces dispositions qui sont de nature à garantir la confidentialité des transmissions n'appellent pas d'observation particulière de la part de la Commission.

Compte tenu de ces observations, **émet un avis favorable** au projet de décret présenté par le ministre de la Jeunesse et des Sports fixant les modalités de la transmission de données individuelles prévues à l'article L. 3622-6 du Code de la santé publique et les garanties du respect de l'anonymat des personnes qui s'y attachent.

Délibération n° 02-020 du 21 mars 2002 sur un projet d'arrêté relatif à la notification obligatoire des infections aiguës symptomatiques par le virus de l'hépatite B et des infections par le virus de Pimmunodéficience humaine

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre de l'Emploi et de la Solidarité d'un projet d'arrêté relatif à la notification obligatoire des infections aiguës symptomatiques par le virus de l'hépatite B et des infections par le virus de l'immunodéficience humaine ;

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

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

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

Vu le Code de la santé publique et notamment son article L. 3113-3 ;

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

Vu le décret n° 2001-437 du 16 mai 2001 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies visées à l'article L. 3113-1 du Code de la santé publique et modifiant les articles R. 11-2 et R. 11-3 du Code de la santé publique ;

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

Formule les observations suivantes :

Le projet d'arrêté relatif à la déclaration des infections aiguës symptomatiques par le virus de l'hépatite B et des infections par le virus de l'immunodéficience humaine est pris en application des dispositions du décret n° 2001-437 du 16 mai 2001 sur lequel la Commission s'est prononcée par une délibération n° 00-45 du 3 octobre 2000.

Ce décret prévoit que pour chacune des maladies à déclaration obligatoire un arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les informations destinées à la surveillance épidémiologique et, en particulier les données cliniques, biologiques et socio-démographiques que le médecin déclarant ou, en cas de diagnostic biologique, le médecin prescripteur porte sur la fiche de notification.

La Commission prend acte que l'article 3 du projet d'arrêté subordonne son entrée en vigueur à la mise en place effective par l'Institut de veille sanitaire, organisme chargé de gérer l'application informatique de surveillance du VIH et de l'hépatite B, du système de codage informatique destiné à garantir l'anonymat des personnes et qui doit, conformément aux dispositions du décret précité, être irréversible et constitué à partir des trois premières lettres du nom, du prénom, de la date de naissance et du sexe de la personne.

S'agissant des variables démographiques :

Le projet prévoit, au titre des variables démographiques appelées à figurer sur le formulaire de notification de l'infection par le VIH, l'année de naissance, le sexe, le département ou le pays de domicile (sous la forme : France ou étranger), le pays de naissance, la nationalité à la naissance et la nationalité actuelle. Il est précisé que les mentions du pays de naissance, de la nationalité à la naissance et de la nationalité actuelle doivent permettre de caractériser les problèmes de santé spécifiques des personnes étrangères atteintes par le VIH ou par le virus de l'hépatite B vivant en France.

La Commission estime cependant que les données relatives au pays de naissance, au pays de domicile et à la nationalité actuelle constituent des indicateurs suffisants au regard de la finalité du traitement et des exigences épidémiologiques, sans qu'il soit nécessaire que le professionnel de santé ait à interroger en outre les personnes concernées sur leur nationalité à la naissance, information supplémentaire dont le recueil n'entre pas dans l'exercice habituel de l'activité professionnelle des médecins et qui apparaît excessive au regard de la finalité poursuivie.

S'agissant de la profession de la personne, il est prévu qu'elle sera collectée sur le formulaire de notification de manière précise. Il est également envisagé de recueillir une information sur le statut d'emploi sous la forme de l'exercice d'une activité ou non. Dans ce dernier cas, une distinction serait opérée selon que la personne est étudiante, en formation, ou effectue son service militaire. Enfin, il serait distingué selon que la personne est en situation d'invalidité ou pensionné, retraité, chômeur ou autre. Il est attendu de l'ensemble de ces informations qu'il permette de mieux connaître les caractéristiques sociales des personnes atteintes par le virus et de mesurer leur degré de précarité.

La Commission rappelle que lors de sa délibération du 9 décembre 1999 portant adoption d'un rapport relatif aux modalités d'informatisation de la surveillance épidémiologique du sida, elle avait estimé que s'il était effectivement utile de mieux connaître les catégories de situations socio-professionnelles des personnes, sur le plan épidémiologique, afin, en particulier, de mieux cibler les actions de prévention, il convenait dans le souci d'éviter toute réidentification possible des personnes concernées de n'enregistrer la profession que sous la forme de catégorie socio-professionnelle et non de manière précise.

Il a cependant été fait valoir que l'utilisation par les médecins déclarants de la nomenclature de l'INSEE, divisée en trente catégories, était susceptible d'entraîner des erreurs de codage et de remettre ainsi en cause la fiabilité de ce recueil d'informations et qu'il apparaissait préférable que la codification soit réalisée, de façon harmonisée, par les techniciens spécialisés de l'Institut de la veille sanitaire (InVS), à partir de l'indication en clair de la profession.

La Commission estime que l'indication sur le formulaire de notification de la profession peut être admise à la double condition qu'il soit procédé, lors de la saisie informatique des déclarations, à la codification de cette information selon une nomenclature de catégories socio-professionnelles évitant tout risque de réidentification et que la confidentialité des déclarations soit parfaitement assurée lors de leur transmission aux DDASS et à l'InVS. La demande d'autorisation qui sera présentée par l'InVS pour la mise en œuvre du traitement informatique des déclarations obligatoires devra à cet égard apporter toutes les précisions techniques nécessaires.

Dans ces conditions et sous ces réserves, il peut être admis que le formulaire de notification comporte la profession précise des personnes concernées.

Enfin, la référence au service militaire paraît inadéquate dans la mesure où les modalités d'accomplissement du service national ont été modifiées par la loi portant réforme du service national du 28 octobre 1997.

S'agissant des variables biologiques :

Les variables biologiques seraient relatives aux sérologies antérieures négatives et positives, au nombre total de sérologies réalisées, à la date de prélèvement, au type de virus et au profil de séroconversion. Ces données seraient complétées d'informations sur le ou les motifs de dépistage et le stade clinique de l'infection.

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

Le mode et la date de contamination probable, variables fondamentales pour la surveillance de l'infection VIH, seraient collectés de même que des informations sur la nature des rapports sexuels et l'usage de drogues injectables.

Le formulaire comporterait également une rubrique sur le partenaire à l'origine probable de la contamination. Il serait ainsi demandé si le partenaire vit ou a vécu dans une communauté où la prévalence est élevée (Afrique sub-saharienne, Caraïbes, Asie du sud et du sud-est, autre). Cette information permettrait de caractériser le mode de contamination qui constitue l'élément fondamental de la surveillance.

La Commission prend acte que la collecte de ces informations est justifiée par la nécessité d'une part de déterminer si les partenaires ont vécu ou séjourné dans des pays qui connaissent une forte épidémie de sida et où la transmission hétérosexuelle du virus est actuellement prédominante et d'autre part ; de pouvoir définir ainsi l'origine du virus dans la mesure où il peut exister des types de virus différents selon les zones géographiques.

Enfin, les coordonnées du prescripteur et du biologiste seront collectées aux fins de validation des cas et de retour d'information aux déclarants.

Le formulaire de notification de l'hépatite B aiguë répond aux mêmes caractéristiques que celui du VIH s'agissant du codage des données d'identification puisque ce système sera commun à l'ensemble des maladies à déclaration obligatoire.

La Commission estime que les données propres aux facteurs de risque potentiels et aux données biologiques collectées n'appellent pas d'observations particulières.

Estime que le formulaire de déclaration des cas d'infections par le virus de l'immuno-déficience humaine devrait être modifié de façon à supprimer l'indication de la mention relative à la nationalité de naissance ainsi que la référence au service militaire.

Rappelle que le dispositif de notification des données individuelles concernant les cas d'infections aiguës, symptomatiques par le virus de l'hépatite B et les cas d'infections par le virus de l'immuno-déficience humaine, quel que soit le stade, ne peut être mis en œuvre que si toutes les mesures sont prises pour garantir l'anonymat des personnes concernées.

Prend acte à cet égard que ce dispositif demeure subordonné à la mise en œuvre, par l'Institut de veille sanitaire, du système de codage informatique des données d'identification dont le descriptif détaillé devra être soumis à la Commission dans le cadre de la demande d'autorisation du traitement qui sera présenté par l'InVS en application du chapitre V bis de la loi du 6 janvier 1978.

Rappelle que le dossier présenté à l'appui de cette demande devra également décrire, de façon précise, les mesures de sécurité tant physiques que logiques prévues pour garantir l'anonymat des données transmises et traitées.

Délibération n° 02-021 du 2 avril 2002 sur un projet de décret relatif aux conditions dans lesquelles l'Institut de veille sanitaire accède aux informations couvertes par le secret médical et industriel et modifiant le Code de la santé publique

La Commission nationale de l'informatique et des libertés ;

Saisie par la ministre de l'Emploi et de la Solidarité d'un projet de décret relatif aux conditions dans lesquelles l'Institut de veille sanitaire accède aux informations couvertes par le secret médical et industriel et modifiant le Code de la santé publique ;

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

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

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

Vu le Code de la santé publique et notamment ses articles L. 1413-2 à L. 1413-5 et L. 1413-13 ;

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

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

Formule les observations suivantes :

Il est prévu, aux termes de l'article L. 1413-5 du Code de la santé publique issu de la loi sur la veille sanitaire du 1er juillet 1998, que *« à la demande de l'Institut de veille sanitaire, lorsqu'il s'avère nécessaire de prévenir ou de maîtriser des risques pour la santé humaine, toute personne physique ou morale est tenue de lui communiquer toute information en* sa possession *relative à de tels risques. L'Institut accède, à sa demande, aux informations couvertes par le secret médical ou industriel dans des conditions préservant la confidentialité de ces données à l'égard des tiers. »*

L'article L. 1413-13 prévoit qu'un décret en Conseil d'Etat détermine les conditions dans lesquelles l'institut accède à ces informations.

L'institut de veille sanitaire, établissement public administratif placé sous la tutelle du ministre de la santé est chargé, conformément aux dispositions de l'article L. 1413-2 du Code de la santé publique, d'effectuer la surveillance et l'observation permanente de l'état de santé de la population, d'alerter les pouvoirs publics, notamment les agences sanitaires, en cas de menace pour la santé publique, quelle qu'en soit l'origine, et de leur recommander toute mesure ou action appropriée. Il lui appartient également de mener toute action nécessaire pour identifier les causes d'une modification de l'état de santé de la population, notamment en situation d'urgence.

À cet effet, il lui incombe, aux termes de la loi, de recueillir et d'évaluer, le cas échéant sur place, l'information sur tout risque susceptible de nuire à la santé de la population, de participer à la mise en place, à la coordination et, en tant que de besoin, à la gestion des systèmes d'information et à la cohérence du recueil des informations.

La qualité de tiers autorisé, au sens de la loi du 6 janvier 1978, à accéder à de telles informations ainsi reconnues par la loi à l'Institut de veille sanitaire lui permet d'accéder à toute information couverte par le secret médical ou industriel dans les cas où il s'avère nécessaire de prévenir ou de maîtriser des risques pour la santé humaine par exemple, dans des situations avérées d'épidémie ou d'exposition à un risque physique, chimique ou biologique, ou dans une situation de risque potentiel mis en évidence par des études scientifiques ou à la suite d'un événement accidentel ou épidémique.

Il doit être relevé que l'article R. 792-2-1 du projet de décret précise que toute communication d'information à l'Institut de veille sanitaire doit faire l'objet d'une demande écrite et motivée de la part de son directeur général. La demande ainsi formulée doit mentionner le nom, ainsi que l'adresse administrative et électronique de la personne à laquelle ces informations seront transmises. Seul un professionnel de santé pourra être désigné s'il s'agit d'informations de nature médicale. La demande devra également mentionner la durée prévisible de conservation de ces informations. L'article R. 792-2-1 du projet de décret prévoit en outre que la demande doit être satisfaite sans délai, dans des conditions permettant d'en garantir la confidentialité. Ainsi lorsque ces informations seront transmises par voie postale, elles devront être adressées sous double enveloppe, celle placée à l'intérieur devant porter la mention « secret médical » ou « secret industriel ».

La possibilité d'une transmission par voie électronique de ces informations, sous réserve du respect des dispositions de la loi du 6 janvier 1978 et de l'utilisation du dispositif de signature électronique par le destinataire de la demande conformément aux dispositions de l'article 1316-4 du Code civil précisées par le décret du 30 mars 2001 est également prévue par le projet de décret.

S'il convient de prendre acte de la référence faite aux dispositions de la loi du 6 janvier 1978, il y a lieu de relever que l'exigence du recours à un procédé de signature électronique pour télétransmettre les données pourrait s'avérer peu compatible avec le contexte d'urgence de santé publique dans lequel pourront s'inscrire les demandes formulées par l'Institut de veille sanitaire alors que ces procédés restent aujourd'hui difficiles à mettre en œuvre. En tout état de cause, la Commission estime nécessaire, dans la mesure où ces transmissions électroniques de données concerneront des informations médicales nominatives et où la loi impose que la confidentialité soit assurée à l'égard des tiers, qu'elles fassent l'objet d'un chiffrement. Ainsi y-a-t'il lieu de préciser, au quatrième alinéa de l'article R. 792-2-1, que les informations peuvent également être adressées sous forme chiffrée par télétransmission.

Les conditions de conservation des données sont précisées par l'article R. 792-2-2 du projet de décret qui indique également qu'à l'issue du délai estimé nécessaire par le directeur de l'InVS pour atteindre les finalités ayant justifié la collecte et le traitement des données, celles-ci seront archivées dans des conditions de nature à garantir leur confidentialité. Celles d'entre elles qui sont couvertes par le secret médical, c'est-à-dire qui sont nominatives seraient préalablement rendues anonymes quel que soit leur mode d'exploitation, papier ou numérique. Cependant, les données nominatives traitées dans le cadre d'une application informatique ne pouvant être conservées que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées et dans les conditions définies par la loi du 6 janvier 1978, la deuxième phrase de l'article R. 792-2-2 devrait être supprimée en ce qu'elle fait référence au directeur général de l'Institut comme seule autorité habilitée à fixer le délai de conservation des données.

L'article R. 792-2-3 du projet de décret prévoit que dans les cas où il serait nécessaire d'alerter les pouvoirs publics d'une menace pour la santé imposant la mise en place de mesures d'urgence individuelles ou collectives, le ministre chargé de la Santé ou les autorités mentionnées au 2° de l'article L. 1413-2 du Code de la santé publique peuvent être destinataires de données couvertes par le secret médical ou industriel dans les conditions décrites précédemment.

La Commission prend acte de ces dispositions qui ont pour effet de conférer, dans certaines hypothèses et sous certaines conditions, la qualité de tiers autorisé, au sens de la loi du 6 janvier 1978, au ministre chargé de la Santé et aux autorités mentionnées au 2° de 'article L. 1413-2 du Code de la santé publique.

Estime que le quatrième alinéa de l'article R. 792-2-1 du projet de décret relatif aux conditions dans lesquelles l'Institut de veille sanitaire accède aux informations couvertes par le secret médical et industriel devrait prévoir que lorsque les données sont transmises par télétransmission, elles doivent être chiffrées.

Considère que l'exigence du recours à un procédé de signature électronique pour télétransmettre les données demeure aujourd'hui peu compatible avec le contexte d'urgence de santé publique dans lequel peut s'inscrire les demandes de l'Institut de veille sanitaire.

Propose de supprimer à la deuxième phrase de l'article R. 792-2-2 du projet de décret la référence au directeur général de l'Institut comme seule autorité habilitée à fixer le délai de conservation des données.

Délibération n° 02-024 du 23 avril 2002 relative à la mission de vérification sur place effectuée auprès de la société CEGEDIM

La Commission nationale de l'informatique et des libertés ;

Ayant procédé, en application de l'article 21 de la loi du 6 janvier 1978, à une mission de vérification sur place auprès de la société CEGEDIM, afin de contrôler les modalités de mise en œuvre des différents traitements automatisés d'informations nominatives des données transmises par les professionnels de santé ;

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

Vu la directive n° 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, et notamment son article 8 ;

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

Vu les articles 226-13 et 226-14 du Code pénal relatifs au secret professionnel ;

Vu le code de la santé publique, et notamment son article L. 4113-7 ;

Vu la déclaration n° 271306 relative à la mise en œuvre, par la société BKL consultant du groupe CEGEDIM, de l'application Doc'ware-Thalès ;

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

Vu la délibération n° 01-010 du 22 février 2001 décidant une mission de vérification sur place auprès de la société CEGEDIM ;

Vu le rapport relatif à la mission de contrôle adressé par lettre du 21 décembre 2001 et les observations en réponse de la société CEGEDIM reçues par lettres du 17 janvier 2002 et du 15 avril 2002 ;

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

Formule les observations suivantes :

L'application Doc'ware-Thalès, mise en œuvre par la société BKL consultant du groupe CEGEDIM, est une base de données médicales alimentée par des informations télé-transmises par un échantillon de médecins, dotés à cet effet gratuitement (depuis le début des années 90) par cette société d'un équipement informatique et d'un logiciel, dénommé Doc'ware. La diffusion auprès des médecins de cette application évolue vers un système payant du logiciel Doc'ware et de l'équipement informatique, l'offre comprenant également un service de maintenance et de mise à jour.

Ce logiciel permet au médecin de gérer le fichier de ses patients, d'éditer automatiquement ordonnances, certificats, lettres aux confrères, feuilles de soins, de gérer sa comptabilité, de disposer de bases de données sur les médicaments. Il comprend également un module, optionnel, de télétransmission des feuilles de soins.

Une clause du contrat conclu entre la société BKL consultant et les médecins se dotant du logiciel Doc'ware informe ces derniers de « *la communication de certaines informations anonymes, précisées en annexe, à la société, à des fins d'utilisation statistique par cette dernière dans le cadre de diffusion de ses études en épidémiologie et santé publique* ».

La déclaration, adressée en 1989 à la Commission pour la mise en œuvre de cette application, précisait qu'aucune donnée nominative sur les patients n'était transmise et que seules des données statistiques, agrégées et anonymes, étaient commercialisées. La Commission, après avoir obtenu des garanties quant aux conditions d'extraction et de télé-transmission des données, a délivré un récépissé, conformément aux dispositions de l'article 16 de la loi du 6 janvier 1978.

Le contrôle entrepris avait pour objet de vérifier sur place les modalités d'extraction et de télétransmission des informations, ainsi que les conditions d'exploitation par la société BKL consultant du groupe CEGEDIM de ces données, afin, notamment, de s'assurer du caractère anonyme des données relatives aux patients et de la compatibilité du dispositif pris dans son ensemble avec les dispositions de l'article L. 4113-7 du Code de la santé publique, qui interdisent *« la constitution et l'utilisation à des fins de prospection ou de promotion commerciale de fichiers composés à partir de données issues directement ou indirectement des prescriptions […] dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur »*.

Sur le respect de l'anonymat des patients

Les données sont transférées sous un « numéro du patient », composé d'un numéro identifiant le médecin (numéro séquentiel attribué par la société BKL consultant du groupe CEGEDIM) et d'un numéro séquentiel, attribué par le logiciel mis à la disposition du médecin, au fur et à mesure de l'inscription de nouveaux patients dans son fichier médical, ce qui permet de « chaîner » les informations relatives à un même patient chez un même médecin, et donc de suivre sa prise en charge sur la durée.

Pour ce qui concerne le patient, sont télé-transmises les données relatives au sexe, à l'année de naissance (le mois de naissance est précisé pour les enfants de moins de trois ans), au numéro du département de domicile, au « contexte familial » (qui recouvre la situation familiale et le nombre d'enfants) — donnée qui n'est toutefois pas exploitée —, à la catégorie socio-professionnelle — remplie imparfaitement —, à l'existence d'un régime alimentaire — donnée non exploitée —, au fait qu'il s'agit d'une visite à domicile.

S'agissant des données relatives à la consultation du jour, sont transmis la date et les motifs de consultation, les symptômes ou signes cliniques ou de crises, le diagnostic, l'indication éventuelle d'un accident du travail ou d'une maladie professionnelle, les antécédents et facteurs de risque, (ex. existence d'allergies, hérédité cardio-vasculaire, situation de ménopause), pour certaines pathologies l'indice de gravité, les actes paramédicaux, les vaccins pratiqués.

Sont également communiquées les données de prescription (le libellé du médicament, son code CIP, le nom du laboratoire fabriquant, son prix unitaire, son taux de remboursement, la posologie), l'indication éventuelle d'un traitement de fond, d'un renouvellement, d'un traitement prescrit à l'origine par l'hôpital ou par un spécialiste, le motif de suppression d'un médicament antérieurement prescrit. Enfin, les résultats d'examens complémentaires, sous forme de valeurs chiffrées, pour les cholestérol, glycémie, triglycémie, sont transmis — mais actuellement peu exploités, car imparfaitement renseignés. Les résultats de sérologie HIV ne sont pas transmis.

Les données à télé-transmettre sont automatiquement enregistrées, au jour le jour, dans un répertoire du disque dur du poste de travail du médecin. Pour envoyer les données à l'Observatoire Thalès, le médecin doit activer la fonction « transmission » du logiciel. Une procédure automatique sur le poste du médecin déclenche, à une heure programmée, la connexion au serveur de la société CEGEDIM et l'interrompt quand la transmission est terminée.

Si les nom, prénoms et adresse des patients ne sont pas télé-transmis par le médecin, et si les informations télé-transmises ne sont pas, en tant que telles, de nature à permettre à cette société d'identifier le patient concerné, il demeure que l'association de ces données avec un « numéro de patient », attribué par le médecin, télé-transmis à la société BKL consultant du groupe CEGEDIM, et inclus tel quel dans les traitements d'exploitation mis en oeuvre par cette société, ne garantit pas que l'anonymat du patient soit préservé en toutes circonstances, alors que, de surcroît, la société CEGEDIM assure la maîtrise totale de l'ensemble des fonctionnalités du logiciel ainsi que de la procédure d'extraction des données depuis le fichier local du médecin en procédant à la récupération du fichier de télétransmission conservé sur le poste de travail de ce dernier.

La Commission estime que, pour que la parfaite confidentialité des données relatives aux patients soit garantie, les données médicales enregistrées dans les fichiers locaux des médecins devraient être chiffrées, et que le dispositif repose sur une clé de cryptage ne devant être connue que du seul médecin. Seule l'adoption d'une telle mesure serait de nature à éviter les risques de divulgation de données nominatives ou d'intrusion dans le fichier local du médecin. À défaut de recourir à une telle solution, la société BKL consultant du groupe CEGEDIM devrait alors mettre en œuvre les dispositifs de contrôle nécessaires pour garantir que le logiciel mis à disposition de chaque médecin est conforme à la déclaration effectuée auprès de la CNIL.

En tout état de cause, et dans l'attente d'une solution en ce sens, il convient que le numéro identifiant le patient, tel qu'il est enregistré dans la base d'exploitation de la société BKL consultant du groupe CEGEDIM, soit différent du numéro produit par le poste de travail du médecin. La mise en œuvre, à la diligence de la société CEGEDIM, sur le poste de travail des médecins affiliés, d'une fonction de type « hachage » avec clé secrète, créant un nouveau numéro de patient lors de l'extraction des données, serait de nature à satisfaire à cette exigence de sécurité destinée à garantir le secret médical, lequel devrait en outre être renforcé par le chiffrement des données ainsi télé-transmises.

Sur la conformité du dispositif dans son ensemble aux prescriptions de l'article L 4113-7 du Code de la santé publique

L'ensemble des données médicales télé-transmises vient enrichir la base de données centrale Thalès. Ces données sont conservées pendant quatre à cinq ans, à des fins de requêtes pour la production des statistiques par le service des études.

En flux retour, Thalès adresse au médecin des messages. Au nombre de ceux-ci figurent des campagnes de publicité commercialisées par la société CEGEDIM pour le compte des laboratoires de l'industrie pharmaceutique, sous la forme de « spots » d'environ trente secondes chacun apparaissant alors sur l'« économiseur » d'écran du médecin, la publicité ainsi opérée l'étant sans profilage préalable du médecin.

Le service des études qui est chargé d'établir des tableaux statistiques, en vue d'évaluer l'activité et les prescriptions des médecins, dispose donc de l'ensemble des informations transmises, ces informations étant associées, non pas à l'identité du médecin concerné, mais à un numéro d'identification du médecin, lequel est cependant utilisé par ailleurs par d'autres services de la société CEGEDIM. Un responsable (le « directeur des panels ») dispose d'une table de correspondance entre ce numéro et l'identité du médecin.

À l'inverse, le service informatique, les services administratifs et commerciaux de la société ont connaissance de l'identité des médecins affiliés, mais ne sont pas habilités à avoir accès aux fichiers contenant les données de prescriptions médicales.

Si un tel dispositif est de nature à éviter que le service des études n'ait connaissance des prescriptions médicales des médecins sous une forme directement nominative à leur égard, sa compatibilité avec les dispositions du Code de la santé publique nécessite que l'identifiant du médecin utilisé par le service des études statistiques ne puisse pas, serait-ce indirectement, permettre l'identification du professionnel concerné.

Pour assurer le respect de l'article L. 4113-7 du Code de la santé publique, la Commission estime que la société CEGEDIM doit mettre en œuvre un cloisonnement entre la base de données des études statistiques et les autres fichiers, par l'utilisation d'un identifiant spécifique du médecin, propre au service des études statistiques, procéder au chiffrement de la table de correspondance entre le numéro d'identification utilisé par le service des études statistiques et l'identité des médecins concernés et isoler du réseau interne le poste de travail du responsable de cette table de correspondance.

Prend acte des engagements de la société CEGEDIM :
1) de procéder au chiffrement de la base de données nominatives du médecin, par « recours aux fonctions de chiffrement propres à la base de données Oracle (version 8i) » ;
2) d'établir un cloisonnement entre le fichier des patients du médecin et la base de données Thalès, « *en introduisant une fonction de type "hachage", avec clé secrète, entraînant la régénération des numéros de la base de patients du médecin pour en affecter de nouveaux aux patients* », avec la possibilité, pour le seul médecin, de revenir à l'identité d'un patient pour « *vérifier les* données de certains dossiers... sous *contrôle du médecin par le même processus que celui qui lui permet d'entrer dans le logiciel (authentification par carte CPS ou bien utilisation du n° ADELI associé au mot de passe du médecin) »* ;
3) d'assurer la confidentialité des télé-transmissions vers la société CEGEDIM, en pro cédant au « cryptage des données sur le poste du médecin avant transmission et décryptage sur les serveurs de CEGEDIM à réception » ;
4) d'assurer un confinement de la base Thalès au sein de la société CEGEDIM, par la mise en œuvre d'un système permettant *« de découpler la numérotation des méde cins participant à l'observatoire épidémiologique entre, d'une part, l'ensemble du système permettant tant de gérer les données transmises que de les traiter pour pro duire les études Thalès, et, d'autre part, l'ensemble du système "amont" à caractère commercial » ;*
5) de chiffrer le poste de travail du directeur des panels, par recours *« aux outils four nis par la société MSI pour permettre un chiffrement du contenu de ce poste »* ;
6) d'isoler du réseau interne de la CEGEDIM le poste de travail du directeur des panels.

Demande :
— afin de mieux garantir l'anonymat du patient, que la société CEGEDIM mette en œuvre un chiffrement du fichier local de chaque médecin reposant sur une clé de cryptage secrète connue du seul médecin ;
— qu'au titre de la loyauté du contrat passé entre le médecin et la société CEGEDIM, les médecins soient en mesure de visualiser, à leur initiative, sous forme de texte en clair — et non sous forme codée — les informations destinées à être télé-transmises ;
— que la société CEGEDIM adresse à la CNIL, avant le 1er octobre 2002, les élé ments techniques de nature à lui permettre de s'assurer que les engagements pris par la société ainsi que les demandes précitées sont effectivement mises en œuvre.

Décide de procéder à un contrôle après un délai d'un an.

Délibération n° 02-082 du 19 novembre 2002 sur une demande d'autorisation présentée par l'Institut national de veille sanitaire concernant la mise en place de l'application informatique destinée à la surveillance épidémiologique nationale des maladies infectieuses à déclaration obligatoire dont le VIH/sida, et sur un projet d'arrêté présenté par le ministre de la Santé relatif à la notification obligatoire des maladies infectieuses visées à l'article D. 11-1 du Code de la santé publique

La Commission nationale de l'informatique et des libertés ;

Saisie pour autorisation par le directeur général de l'Institut national de la veille sanitaire de la mise en place de l'application informatique destinée à la surveillance épidémiologique nationale des maladies infectieuses à déclaration obligatoire dont le VIH/sida ;

Saisie pour avis par le ministre de la santé d'un projet d'arrêté relatif à la notification obligatoire des maladies infectieuses visées à l'article D. 11-1 du Code de la santé publique ;

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

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

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

Vu le Code de la santé publique et notamment son article L. 3113-3 ;

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

Vu le décret n° 2001-437 du 16 mai 2001 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies visées à l'article L. 3113-1 du Code de la santé publique et modifiant les articles R. 11-2 et R. 11-3 du code de la santé publique ;

Vu les saisines effectuées par l'Institut de veille sanitaire auprès du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé ;

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

Formule les observations suivantes :

Le directeur général de l'Institut national de veille sanitaire (InVS) soumet à la Commission une demande d'autorisation concernant l'application informatique destinée à gérer la surveillance épidémiologique des maladies infectieuses à déclaration obligatoire.

L'article L. 3113-1 du Code de la santé publique dispose en effet que les maladies qui nécessitent une intervention urgente locale, nationale ou internationale et les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique font l'objet d'une transmission obligatoire de données

individuelles à l'autorité sanitaire. En outre, la loi prévoit que les modalités de transmission des données et, en particulier la manière dont l'anonymat est protégé, sont fixées par décret en Conseil d'État.

La Commission est également saisie par le directeur général de la santé d'un projet d'arrêté relatif à la notification obligatoire des maladies infectieuses pris en application des dispositions du décret du 16 mai 2001 fixant les modalités de transmission à l'autorité sanitaire de données individuelles concernant les maladies à déclaration obligatoire.

Sur la nature des informations nécessaires à la notification

Les articles R. 11-2 et suivants du Code de la santé publique issus du décret du 16 mai 2001 énumèrent les informations qui doivent figurer sur la fiche de notification des données individuelles et, en particulier, l'exigence d'un numéro d'anonymat établi par codage informatique irréversible à partir des éléments d'identité de la personne. C'est également aux termes de ces dispositions, qu'il est prévu que pour chaque maladie à déclaration obligatoire, un arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les informations destinées à la surveillance épidémiologique et, en particulier les données cliniques, biologiques et socio-démographiques que le médecin déclarant ou, en cas de diagnostic biologique, le médecin prescripteur porte sur la fiche de notification.

Ainsi, outre les coordonnées du déclarant qui mentionne son nom, son prénom et son adresse et le numéro d'anonymat propre à la personne, les informations sont relatives à la date des premiers signes cliniques de la maladie, à la date et au lieu d'hospitalisation, aux signes cliniques et résultats biologiques permettant de déterminer si les critères de déclaration sont remplis, à l'évolution de la maladie, aux facteurs de risque, aux antécédents de prophylaxie et aux éléments permettant de déterminer une exposition ou un mode de transmission.

En ce qui concerne l'infection par le VIH/sida et les infections aiguës symptomatiques par le virus de l'hépatite B, la Commission s'est déjà prononcée par délibération du 21 mars 2002. Elle prend acte de l'abaissement à l'âge de treize ans pour la définition de la maladie du sida.

La nature de ces informations n'appelle pas d'observations particulières de la part de la Commission.

Sur la garantie de l'anonymat

Il appartient à l'Institut national de veille sanitaire, établissement public chargé de la surveillance de l'état de santé de la population, de garantir l'anonymat des personnes concernées, tel que défini à l'article L. 3113-1 du Code de la santé publique.

La procédure d'anonymisation mise en œuvre sera double et irréversible. Ainsi, une première anonymisation sera effectuée au niveau local, par les laboratoires pour la notification des infections par le virus de l'immunodéficience humaine et pour les infections aiguës symptomatiques par le virus de l'hépatite B, par les médecins hospitaliers pour le sida et par les directions départementales des affaires sanitaires et sociales pour les maladies à déclaration obligatoire qui, conformément aux dispositions de l'article L. 3113-1 du Code de la santé publique, nécessitent une intervention urgente locale, nationale ou internationale. Elle sera réalisée au moyen d'un logiciel de hachage qui permettra de générer, à partir de la première lettre du nom de la personne, de son prénom, de sa date de naissance et de son sexe, un numéro d'anonymat sous forme d'une chaîne de seize caractères en majuscules.

Une deuxième anonymisation sera réalisée au niveau national par l'Institut national de veille sanitaire à partir de l'identifiant et d'une clé secrète détenue par l'InVS. Cette opération permettra de couper tout lien entre la personne et les données la concernant.

La Commission estime que cette technique de double anonymisation est de nature à satisfaire aux exigences de confidentialité dans la mesure où elle s'accompagne de mesures de sécurité efficaces.

Sur le circuit de notification et les mesures de sécurité

Les modalités de transmission des données individuelles nécessaires à la surveillance épidémiologique sont différentes selon qu'il s'agit de l'infection par le VIH/sida, des infections aiguës symptomatiques par le virus de l'hépatite B et des autres maladies à déclaration obligatoire.

En cas de diagnostic d'infection à VIH chez l'adulte et l'adolescent de 13 ans et plus ou d'hépatite B aiguë, il appartient au biologiste d'établir le code d'anonymat du patient et d'adresser un premier feuillet, complété d'éléments sur la sérologie effectuée et le diagnostic de l'infection, au médecin inspecteur de santé publique de la direction départementale des affaires sanitaires et sociales de son lieu d'exercice. Deux autres feuillets de la fiche de notification qui portent le code d'anonymat et qui ne doivent pas être détachés seront adressés au médecin prescripteur, avec les résultats du dépistage. Le biologiste conservera pendant six mois un quatrième feuillet qui est un duplicata du premier.

Dans un deuxième temps, le médecin prescripteur après avoir complété son feuillet des éléments relatifs notamment au stade clinique de l'infection et aux modes de contamination probables, l'adressera au médecin inspecteur de la DDASS de son lieu d'exercice.

Pour les cas d'infection VIH et sida chez l'enfant de moins de 13 ans et pour la notification des cas de sida chez l'adulte, il appartient au médecin d'établir le code d'anonymat de la personne. Il complète le feuillet de la fiche de notification des éléments de diagnostic et l'adresse au médecin inspecteur de santé publique de la DDASS de son lieu d'exercice.

Afin de garantir la confidentialité des données, seul le médecin prescripteur conservera la table de correspondance entre l'identité du patient et le code d'anonymat pour l'ensemble des notifications VIH, sida et hépatite B aiguë pendant six mois.

S'agissant des notifications d'infection VIH chez l'adulte et l'adolescent de 13 ans et plus et d'hépatite B aiguë, le médecin inspecteur de santé publique de la DDASS couple les feuillets du biologiste et du médecin à l'aide du numéro d'anonymat. Pour les notifications des cas d'infections VIH chez l'enfant de moins de 13 ans et des cas de sida, il ne reçoit que le seul feuillet émanant du médecin déclarant.

Après avoir procédé à la validation des fiches, le médecin inspecteur de santé publique transmet les fiches à l'InVS et les conserve dans des conditions garantissant leur confidentialité.

En ce qui concerne les autres maladies, la notification est effectuée par les médecins et les biologistes de manière indépendante à l'aide d'une fiche de notification composée d'un seul feuillet. Le médecin inspecteur de santé publique, après avoir effectué les contrôles de cohérence, établit le code d'anonymat et transmet les fiches à l'InVS sous double enveloppe comportant une enveloppe externe libellée à l'InVS-DMI (département des maladies infectieuses) et une enveloppe interne libellée à l'attention du médecin responsable du département maladies infectieuses avec la mention « secret médical ». Il conserve la table de correspondance pendant six mois.

L'Institut national de veille sanitaire procédera ensuite à l'enregistrement par ordre chronologique de chaque fiche de notification dès leur réception. Outre le numéro d'enregistrement, seront enregistrées des indications sur la nature de la maladie, la date de déclaration, la date de réception de celle-ci, le numéro du département de la DDASS expéditrice. Le code d'anonymat ne sera pas enregistré.

Les médecins épidémiologistes de l'InVS procéderont, sous le contrôle du médecin responsable au département des maladies infectieuses, à la validation médicale des fiches. C'est lors de la saisie des fiches, qui sera effectuée sur un poste informatique dédié dont l'accès sera protégé par un lecteur de carte et par un « login » et un mot de passe, qu'il sera procédé, à partir du code d'anonymat et de la clé secrète de l'InVS, à une nouvelle anonymisation.

Les mesures de sécurité mises en œuvre à l'InVS qui s'intègrent dans le cadre de la définition d'une nouvelle politique de sécurité paraissent de nature à garantir la confidentialité des données.

Sur *l'information des personnes concernées*

L'Institut de veille sanitaire propose d'élaborer une note individuelle destinée à informer clairement la personne sur le principe de la déclaration obligatoire. Plusieurs rubriques sont prévues : À quoi sert la déclaration obligatoire ? Quelles sont les données qui sont transmises ? A qui ces informations sont-elles destinées ? Comment l'anonymat des personnes est-il protégé ? Comment exercer votre droit d'accès et de rectification ?

Ces documents seront remis au patient par le médecin lors de l'annonce du diagnostic ou au moment qu'il jugera le plus opportun pour la personne. Pour les patients porteurs du VIH/sida, deux autres notes d'information complémentaires sont prévues respectivement pour les parents d'enfants mineurs et pour les adultes.

Le droit d'accès aux informations s'exercera auprès de l'InVS par l'intermédiaire du médecin qui a procédé à la notification et uniquement pendant un délai de six mois après que le médecin a transmis la fiche.

L'ensemble de ces éléments paraît de nature à garantir une information claire et précise des personnes. La commission estime toutefois souhaitable que ces notes d'information soient complétées afin de rappeler que, conformément aux dispositions de la loi du 6 janvier 1978, l'ensemble du dispositif informatique a été autorisé par la CNIL.

Autorise la mise en œuvre par l'Institut national de veille sanitaire de l'application informatique destinée à la surveillance épidémiologique nationale des maladies infectieuses à déclaration obligatoire dont le VIH/sida.

Estime que le projet d'arrêté présenté par le ministre de la santé relatif à la notification obligatoire des maladies infectieuses accompagné des fiches de notification comportant en particulier les données cliniques, biologiques et socio-démographiques nécessaires à la surveillance épidémiologique n'appelle pas d'observation particulière.

Délibération n° 02-053 du 9 juillet 2002 portant avis sur :
— un projet de décret en Conseil d'État présenté par le ministre de l'Économie, des Finances et de l'Industrie pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'INSEE à utiliser le numéro d'inscription au répertoire (NIR) pour le traitement automatisé d'informations nominatives relatif à l'établissement de statistiques comparées sur les valeurs de consommation de soins et de biens médicaux ;
— la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations individuelles relatif à une enquête obligatoire sur la santé et la consommation médicale

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par l'INSEE d'un projet de décret en Conseil d'Etat pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'INSEE à utiliser le numéro d'inscription au répertoire pour le traitement automatisé d'informations nominatives relatif à l'établissement de statistiques comparées sur les valeurs de consommation de soins et de biens médicaux et d'un projet d'arrêté portant création d'un traitement automatisé d'informations individuelles relatif à une enquête obligatoire sur la santé et la consommation médicale ;

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

Vu la directive n° 95/46/CE du Parlement européen et du conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Vu le décret n° 82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques ;

Vu l'arrêté du 11 avril 2002 relatif à la mise en œuvre du système national d'information inter-régimes de l'assurance maladie ;

Vu le projet de décret en Conseil d'État pris en application de l'article 18 de la loi n° 78-17 du 6 janvier 1978 ;

Vu le projet d'arrêté présenté par le directeur général de l'INSEE portant création du traitement automatisé d'informations individuelles relatif à une enquête obligatoire sur la santé et la consommation médicale ;

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

Formule les observations suivantes :

L'INSEE saisit la CNIL d'une demande d'avis concernant la mise en oeuvre d'un traitement automatisé d'informations individuelles relatif à une enquête obliga-

toire sur la santé et la consommation médicale, traditionnellement réalisée tous les dix ans depuis 1960.

Cette enquête à caractère obligatoire, sera réalisée auprès de 16 000 ménages et se déroulera d'octobre 2002 à septembre 2003.

L'enquête a pour objectifs de décrire l'état de santé de la population concernée (morbidité déclarée et indicateurs de santé), d'estimer la consommation annuelle de soins et de prévention et enfin d'associer aux états de santé et aux consommations de soins et de prévention, les données socio-démographiques relatives aux individus et aux ménages interrogés.

Les catégories de données traitées auront trait aux caractéristiques socio-démographiques du ménage, aux conditions de vie et de logement, à la situation économique et sociale, à la protection sociale, aux gênes et difficultés dans la vie quotidienne, à la santé, aux maladies en cours, aux antécédents chirurgicaux, à la consommation de soins et biens médicaux durant deux mois, aux risques professionnels, aux comportements de prévention.

L'INSEE sera le seul destinataire des informations recueillies. Le CREDES disposera d'un fichier anonymisé avec un numéro d'ordre non signifiant pour procéder au codage des maladies et des consommations déclarées lors de l'enquête.

En application des dispositions de l'article 18 de la loi du 6 janvier 1978, l'INSEE souhaite, par ailleurs, être autorisé à collecter le numéro d'inscription au répertoire des personnes interrogées à l'occasion de l'enquête. Cette collecte, facultative, aura pour objet de permettre à la CNAMTS, gestionnaire du système national d'information inter-régimes de l'assurance maladie (SNIIRAM), de rechercher dans cette base les enregistrements correspondant aux consommations de soins et de biens médicaux des personnes objets de l'enquête, dans des conditions garantissant l'anonymat des personnes, afin d'établir des statistiques agrégées sur le volume et la valeur des prestations annuelles d'assurance maladie.

Une comparaison sera ensuite effectuée entre les résultats estimés à partir de l'enquête et les données de l'assurance maladie.

La Commission prend acte de ce que les NIR ainsi obtenus feront l'objet, avant transmission à la CNAMTS, d'une procédure de transcodage par l'INSEE selon les procédures définies par la CNAMTS, lors de la création du SNIIRAM, lesquelles garantissent l'anonymat des bénéficiaires de soins. La CNAMTS, après un deuxième transcodage, obtiendra des numéros à partir desquels, elle recherchera dans le SNIIRAM les consommations correspondant aux numéros listés. Elle adressera à l'INSEE des statistiques agrégées. L'INSEE s'est par ailleurs engagé à détruire la liste des NIR dés la fin du transcodage.

La Commission considère que dans la mesure où la CNAMTS participe à l'opération en utilisant le SNIIRAM le projet de décret en Conseil d'État pris en application de l'article 18 de la loi du 6 janvier 1978 devrait comporter le contreseing du ministre des Affaires sociales, du Travail et de la Solidarité.

Émet, sous cette observation, un avis favorable au projet de décret en Conseil d'Etat pris en application de l'article 18 de la loi du 6 janvier 1978 et autorisant l'INSEE à utiliser le numéro d'inscription au répertoire pour l'établissement de statistiques comparées sur les valeurs de consommation de soins et de biens médicaux, lors de l'enquête santé 2002-2003.

Émet un avis favorable au projet d'arrêté présenté par le directeur général de l'INSEE concernant la création d'un traitement automatisé d'informations individuelles relatif à une enquête obligatoire sur la santé et la consommation médicale.

Délibération n° 02-058 du 17 septembre 2002 portant avertissement à l'association hospitalière du bassin de Longwy

La Commission nationale de l'informatique et des libertés ;

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

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

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

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

Vu la délibération n° 01-025 du 15 mai 2001 de la Commission décidant une mission de contrôle sur place auprès de l'association hospitalière du bassin de Longwy afin de vérifier l'ensemble des mesures de sécurité mises en œuvre pour garantir la confidentialité des données nominatives conservées au sein du département d'information médicale ;

Vu le compte rendu de la mission de vérification sur place adressé le 12 juillet 2002 et les observations en réponse de l'association hospitalière du bassin de Longwy reçues par lettre du 16 août 2002 ;

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

Saisie par le Conseil national de l'ordre des médecins d'une plainte d'un médecin qui, ayant exercé les fonctions de responsable du département d'informations médicales au sein de l'association hospitalière du bassin de Longwy, a fait état d'atteintes à la confidentialité des informations nominatives traitées sur le système informatique de l'hôpital et, en particulier de l'accès, par des personnels administratifs, à des données individuelles recueillies dans le cadre du programme de médicalisation des systèmes d'information (PMSI) mis en place dans les établissements de santé en application des dispositions de l'article L. 6113-7 du Code de la santé publique.

Aux termes de ces dispositions, les médecins sont tenus de transmettre les données médicales nécessaires à l'analyse de leur activité au médecin responsable du département d'informations médicales qui veille à la qualité des données qu'il peut confronter, en tant que de besoin avec les dossiers médicaux et les fichiers administratifs. Ce médecin est soumis dans le cadre de ses fonctions de médecin DIM au respect du secret médical comme le sont les personnels placés ou détachés auprès de lui et qui travaillent à l'exploitation de données nominatives sous son autorité, ainsi que des personnels intervenant sur le matériel et les logiciels utilisés pour le recueil et le traitement des données.

En application de l'article R. 710-5-6 du Code de la santé publique, il appartient au directeur de l'établissement de prendre toutes dispositions utiles avec le médecin responsable de l'information médicale et après avis de la commission médicale d'établissement afin de préserver la confidentialité des données médicales

nominatives. Ces dispositions concernent notamment l'étendue, les modalités d'attribution et le contrôle des autorisations d'accès ainsi que l'enregistrement des accès.

La Commission a décidé, par une délibération du 15 mai 2001, de procéder à une mission de vérification sur place afin de vérifier l'ensemble des mesures de sécurité mises en oeuvre pour garantir la confidentialité des données médicales nominatives traitées et conservées au sein du département d'information médicale.

Cette mission de contrôle s'est déroulée le 6 mars 2002 dans les locaux de l'association hospitalière du bassin de Longwy.

Les investigations de la Commission ont permis de constater que le traitement mis en œuvre au sein de l'établissement pour assurer la fourniture des informations médicales nécessaires dans le cadre du programme de médicalisation des systèmes d'information, est géré par le directeur informatique qui peut ainsi avoir accès à l'application.

S'agissant des mesures de sécurité mises en place, il a été relevé que l'application ne prévoit aucune hiérarchisation des accès et qu'en particulier, la seule possession du mot de passe dont l'attribution et la gestion n'obéissent à aucune règle prédéfinie, permet de consulter l'intégralité du dossier. Il n'existe pas non plus de journalisation des accès tant au système qu'à l'application. Tout utilisateur disposant d'un accès au logiciel sur son poste de travail peut sur simple requête modifier les données de la base sans qu'il soit conservé trace de l'auteur à l'origine de la modification.

La Commission prend acte du fait que la direction de l'hôpital ne nie pas l'insuffisance des mesures de sécurité actuellement mises en oeuvre et reconnaît que l'état du système informatique et les modalités actuelles de son fonctionnement ne permettent pas de répondre aux exigences requises en matière de respect de la confidentialité.

Par courrier du 16 août 2002, le directeur général de l'hôpital a informé la CNIL qu'une nouvelle application informatique de gestion hospitalière sera mise en œuvre et qu'elle apportera les garanties de sécurité indispensables.

La Commission relève par ailleurs, que les autres applications informatiques mises en œuvre au sein de l'hôpital n'ont pas encore fait l'objet de formalités préalables auprès de la CNIL. C'est ainsi le cas des applications sur le suivi des prescriptions en chimiothérapie, du PMSI psychiatrie, de la gestion des ressources humaines et de la gestion du temps de travail des salariés et du PMSI moyen et long séjour.

En conséquence :

Demande à être saisie, dans un délai dé trois mois à compter de la présente délibération, d'une demande d'avis établie conformément à l'article 15 de la loi du 6 janvier 1978 et relative à la mise en place du nouveau système de gestion hospitalière. Les mesures de sécurité retenues pour garantir la confidentialité des données devront être décrites en particulier en ce qui concerne les modalités d'accès aux informations, la politique d'attribution et de composition des mots de passe et les modalités retenues pour assurer une journalisation des connexions.

Demande à être saisie dans les plus brefs délais des demandes d'avis relatives aux applications informatiques d'ores et déjà mises en oeuvre au sein de l'hôpital ainsi que des mesures prises pour améliorer la sécurité tant physique que logique de celles-ci.

Décide, faisant application des dispositions de l'article 21-4° de la loi n° 78-17 du 6 janvier 1978 d'adresser à cet effet un avertissement à l'association hospitalière du bassin de Longwy.

Social

Délibération n° 02-005 du 5 février 2002 portant avis sur un projet de décret relatif à l'organisation de l'assurance des non salariés agricoles contre les accidents du travail et les maladies professionnelles

La Commission nationale de l'informatique et des libertés ;

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

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

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

Vu la loi n° 2001-1128 du 30 novembre 2001 portant amélioration de la couverture des non-salariés agricoles contre les accidents du travail et les maladies professionnelles ;

Vu le Code rural ;

Vu les articles R. 115-1 et R. 115-2 du Code de la Sécurité sociale ;

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

Vu le projet de décret présenté par le ministre de l'Agriculture relatif à l'organisation de l'assurance des non salariés agricoles contre les accidents du travail et les maladies professionnelles ;

Vu le courrier adressé le 1er février 2002 par le directeur de l'exploitation, de la politique sociale et de l'emploi du ministère de l'Agriculture ;

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

Saisie pour avis, par le ministère de l'Agriculture d'un projet de décret relatif à l'organisation de l'assurance des non salariés agricoles contre les accidents du travail et les maladies professionnelles ;

Formule les observations suivantes :

La CNIL est saisie par le ministère de l'Agriculture d'un projet de décret prévu en application de la loi du 30 novembre 2001 portant amélioration de la couverture des non-salariés agricoles contre les accidents du travail et les maladies professionnelles, dont l'entrée en vigueur doit intervenir le 1er avril 2002.

La loi précitée a pour objet d'instituer, au profit des exploitants agricoles, un nouveau régime de protection sociale contre ces risques et, à cet effet, confient aux caisses de Mutualité sociale agricole (MSA) la mission d'assurer le contrôle de l'obligation d'affiliation et le service du contrôle médical, de procéder au classement des exploitations selon les risques et d'aider à l'établissement de la tarification, de mettre en oeuvre la politique de prévention, de centraliser les cotisations et de répartir les ressources entre les organismes assureurs et enfin d'assurer la consolidation des informations relatives au fonctionnement du régime.

Le législateur a également prévu que pourront participer à la gestion du régime, les assureurs qui y auront été autorisés à cet effet par arrêté du ministre de l'Agriculture et les caisses de mutualité sociale agricole, les exploitants agricoles ayant désormais le choix d'adhérer auprès d'un assureur ou d'une caisse. Les relations entre les deux types d'organismes intervenants (organismes privés et caisses de MSA) seront fixées par une convention conclue entre la caisse centrale de mutualité sociale agricole et un regroupement des organismes d'assurance privés, oui doit se créer à cet effet et se doter de la personnalité morale. Cette convention devra être approuvée par arrêté du ministre de l'Agriculture.

Pour assurer la mise en œuvre de ce nouveau dispositif, des échanges d'informations sont nécessaires entre les différents partenaires.

L'article L. 752-14 du Code rural (issu de la loi précitée) prévoit ainsi, en son dernier alinéa que les caisses de mutualité sociale agricole et le groupement (des organismes assureurs privés) sont autorisés à échanger les seules informations nominatives nécessaires au bon fonctionnement du régime, dans des conditions fixées par décret en Conseil d'État pris après avis de la CNIL.

En application de cette disposition, la CNIL est saisie d'un projet de décret dont l'article 9 a pour objet de définir les modalités de communication des informations, d'une part, entre les caisses de mutualité sociale agricole et le groupement et d'autre part, entre les caisses de mutualité sociale agricole et le groupement et la caisse centrale de mutualité sociale agricole.

La Commission observe que ces échanges d'informations nominatives ont pour finalités de permettre aux caisses de mutualité sociale agricole de certifier l'immatriculation des assurés, de vérifier la correcte mise en œuvre des procédures de recouvrement, d'assurer le recouvrement de la CSG et de la CRDS, conformément aux dispositions des articles L. 136-4 et L. 136-5-11 du Code de la Sécurité sociale et d'exercer leur mission de contrôle médical.

Elle prend également bonne note que la transmission, par le groupement et par les caisses de mutualité sociale agricole à la caisse centrale de MSA, dans des conditions garantissant l'anonymat des personnes, de données individuelles d'adhésion et le montant des prestations versées à chaque assuré pour chaque accident du travail ou maladie professionnelle, a pour seul objet d'établir les statistiques agrégées nécessaires, respectivement, à la modulation des cotisations telles que prévue par l'article L. 752-17 du Code rural, et à la définition des orientations de la politique de prévention.

La Commission relève cependant que l'article 9 ne définit pas suffisamment la nature des informations nominatives échangées. Ainsi, elle estime nécessaire que le projet de décret mentionne, outre le NIR des exploitants agricoles et des membres de leurs familles les autres catégories d'informations nominatives (identité, dates et lieu de naissance, situations familiales, activité agricole...) appelées à être transmises aux caisses de mutualité sociale agricole pour assurer la certification des procédures d'immatriculation. De même, les catégories d'informations nominatives (identité, dates et montant des cotisations...) appelées à être transmises aux fins de vérification des procédures de recouvrement des cotisations et de recouvrement de la CSG et de la CRDS devraient être énumérées. Enfin, le projet de décret pourrait utilement mentionner les catégories de données appelées à figurer sur les documents (déclarations d'accidents du travail ou de maladies professionnelles, certificats médicaux, décisions d'accord ou de refus de prise en charge, demandes d'entente préalable...) devant être transmis aux caisses de mutualité sociale agricole pour leur permettre d'exercer leur mission de contrôle médical.

La Commission observe également que l'article 9 devrait indiquer les modalités techniques selon lesquelles ces échanges seront réalisés, en particulier en ce qui concerne le mode de support, papier ou électronique, utilisé pour ces échanges et le recours éventuel à des dispositifs de chiffrement des informations qui s'imposent tout particulièrement dès lors qu'il serait envisagé de transmettre par réseau des données médicales nominatives.

Elle considère en conséquence qu'elle ne peut émettre un avis favorable sur les conditions dans lesquelles les caisses de mutualité sociale agricole et le groupement seront autorisés à échanger les seules informations nominatives nécessaires au bon fonctionnement du régime.

Estime qu'elle ne peut, en l'état, donner un avis favorable au projet de décret présenté par le ministre de l'Agriculture relatif à l'organisation de l'assurance des non salariés agricoles contre les accidents du travail et les maladies professionnelles.

Délibération n° 02-047 du 27 juin 2002 relative au projet de décret présenté par le ministère de l'Intérieur portant modification de l'application de gestion des ressortissants étrangers en France (AGDREF) et à la demande d'avis de la Caisse nationale des allocations familiales relative à l'exploitation de certaines données extraites du fichier AGDREF dans le cadre de son obligation de contrôle de régularité du séjour des personnes étrangères souhaitant bénéficier de prestations familiales

La Commission nationale de l'informatique et des libertés ;

Saisie, d'une part, par le ministère de l'Intérieur d'un projet de décret portant modification du décret du 29 mars 1993 portant création d'un système informatisé de gestion des dossiers des ressortissants étrangers en France (AGDREF) et, d'autre part, par la Caisse nationale des allocations familiales d'une demande d'avis relative à l'exploitation de certaines données extraites d'AGDREF ;

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

Vu la 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 ;

Après avoir entendu Messieurs François Giquel et Maurice Viennois, commissaires, en leur rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

Observe :

Le ministère de l'Intérieur a saisi la Commission d'une demande de modification de l'application nationale de gestion des dossiers des ressortissants étrangers en France (AGDREF) visant à prendre en compte diverses modifications législatives et réglementaires relatives aux conditions d'entrée et de séjour des étrangers en France intervenues depuis la mise en oeuvre de cette application.

L'application de gestion des dossiers des ressortissants étrangers en France (AGDREF), créée par un décret du 29 mars 1993 pris après avis favorable de la Commission, a pour finalités :

— d'améliorer les procédures relatives au règlement de la situation administrative des ressortissants étrangers ;

— d'assurer un mode de fabrication des titres de séjour et des récépissés de demande de délivrance ou de renouvellement de ces titres qui évite les risques de fal sification ;

— de permettre la vérification par les agents de l'autorité du séjour d'un ressortis sant étranger en France ;

— de permettre l'établissement de statistiques selon des modalités fixées par arrêté du ministre de l'Intérieur.

Ces modifications ont pour principal objet de permettre la transmission de données issues du traitement AGDREF à certains organismes sociaux ; le ministère de

l'Intérieur a également souhaité intégrer trois modifications : la gestion et l'édition du titre d'identité républicain et du document de circulation pour étranger mineur ; la gestion des dossiers administratifs individuels et des courriers de l'administration centrale du ministère et ayant trait aux étrangers ; la prise en compte des titres de séjour délivrés sous forme d'étiquette autocollante à apposer sur le passeport.

Sur la transmission à certains organismes sociaux d'informations nominatives issues du fichier AGDREF

La Caisse nationale des allocations familiales et le ministère de l'Intérieur ont saisi la CNIL d'un projet informatisé visant à permettre aux caisses d'allocations familiales d'obtenir communication de certaines données relatives aux titres de séjour des étrangers demandeurs ou bénéficiaires de prestations familiales, ainsi que la loi n° 93-1027 du 24 août 1993 relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France leur en offre la possibilité dans le cadre de leur obligation de contrôle de la régularité du séjour des étrangers souhaitant bénéficier de prestations familiales.

L'interrogation du fichier AGDREF se fera par l'envoi d'un fichier d'appel, comportant des éléments d'identification de la CAF et du demandeur, en particulier son numéro AGDREF, au centre serveur national (CSN) de la CNAF, via le centre informatique régional (CERTI) dont dépend la caisse.

Les demandes d'interrogation provenant des différentes CAF, et contenant exclusivement le numéro AGDREF de la personne concernée, la catégorie d'organisme demandeur (CNAF en l'occurrence) ainsi qu'un numéro de liaison non signifiant attribué par le CSN, seront transmises au moins une fois par mois au ministère de l'Intérieur. L'identification précise de la caisse formant la requête ne sera pas transmise.

Ces demandes seront réceptionnées dans une « boîte aux lettres » informatique afin d'éviter toute intrusion au sein des différents systèmes applicatifs du ministère. Après traitement par le ministère, un fichier « réponse » contenant le code résultat, les nom, prénom, date de naissance, adresse, type de demande, référence réglementaire et le type de document pour les codes « trouvés » et « purgés », sera mis à disposition du CSN.

Le CSN, informé par un avis de mise à disposition, disposera de vingt-quatre heures pour procéder à la récupération du fichier « réponse » au niveau du sas. Passé ce délai, le fichier « réponse » sera effacé, le ministère de l'Intérieur ne conservant aucune trace des interrogations.

Ainsi, le dispositif envisagé ne prévoit pas un accès au fichier AGDREF mais une simple mise à disposition indirecte des données du fichier AGDREF, sur la base du seul numéro AGDREF et pendant un court laps de temps, au bénéfice de la CNAF.

La Commission prend acte de ce que le dispositif technique d'interrogation d'AGDREF a été conçu pour répondre aux seuls besoins des caisses et que le traitement permettant l'extraction d'informations issues du fichier AGDREF et leur rapprochement avec le fichier des CAF ne donnera lieu à aucune exploitation de la part du ministère de l'Intérieur.

La Commission prend également note que la CNAF s'est engagée à ce que les motifs d'interrogation et les résultats des rapprochements avec le fichier AGDREF ne soient pas communiqués aux services préfectoraux.

Le projet d'acte réglementaire de la CNAF prévoit ainsi en son article 5 que « *les résultats des contrôles effectués par interrogation du fichier AGDREF ne feront*

en aucun *cas l'objet d'une transmission aux services préfectoraux ou nationaux du ministère de l'Intérieur ».*

La Commission prend acte de ces différentes garanties qui apparaissent de nature à éviter toute utilisation du fichier « réponse » à des fins autres que celles de contrôle par les organismes sociaux de la régularité du séjour en France des étrangers concernés, mais estime cependant nécessaire, s'agissant de la transmission des codes « archivé » et « purgé » dont l'interprétation nécessiterait un rapprochement avec les services préfectoraux concernés, que le fichier « réponse » du ministère de l'Intérieur indique les motifs de purge ou d'archivage relatifs aux dossiers faisant l'objet d'un contrôle.

L'information des intéressés sera assurée, d'une part, par une mention figurant sur les formulaires du ministère de l'Intérieur permettant l'ouverture et la gestion des dossiers des ressortissants étrangers en France ; cette mention devra être complétée de façon à ce que ces derniers soient, conformément à l'article 27 de la loi du 6 janvier 1978, parfaitement informés de la possibilité offerte aux organismes sociaux de bénéficier, à leur demande, de renseignements relatifs à la régularité de leur situation sur le territoire national.

D'autre part, la CNAF s'est engagée à ce qu'une modification soit apportée aux imprimés de demande de prestations familiales pour mentionner la vérification systématique de la régularité du séjour auprès des services du ministère de l'Intérieur.

Il apparaît toutefois, dans le cas d'une discordance entre les informations connues de la CAF et celles communiquées par AGDREF et dans la mesure où cette discordance aurait une incidence négative sur les droits à prestations, que les droits de l'intéressé seraient modifiés et qu'une notification individuelle, comportant le motif de la décision, lui serait adressée. La CNAF précise également que les usagers auraient la possibilité d'obtenir toute précision utile sur le motif de la décision et, comme à l'accoutumée, de formuler des recours et de bénéficier de remises de dettes.

La Commission estime que, dans la mesure où cette procédure ne lui paraît pas compatible avec les dispositions de la loi du 6 janvier 1978, s'agissant de l'automaticité de la prise de décision à l'égard des allocataires, l'acte réglementaire de la CNAF doit être amendé de façon à préciser que la personne objet du contrôle pourra faire valoir ses observations avant toute prise de décision la concernant et non a *posteriori* comme il est actuellement envisagé.

La Commission prend acte, s'agissant des mesures de sécurité techniques et eu égard à la nature du réseau TRANSPAC, de ce que la CNAF a engagé une réflexion sur de possibles mesures de chiffrement et d'authentification des échanges.

Elle souhaite toutefois que, a minima, un dispositif de chiffrement soit mis en œuvre dans un délai d'un an afin d'assurer la confidentialité des données échangées.

S'agissant des nécessaires mises à jour et apurements du fichier AGDREF, la Commission rappelle au ministère de l'Intérieur les termes de sa délibération du 7 mai 1991 et lui demande de l'informer des mesures adoptées sur ce point.

Sur *les autres modifications du fichier AGDREF*

Ces modifications se limitent à la prise en compte, au plan technique, des évolutions législatives et réglementaires intervenues en matière de conditions d'entrée et de séjour des étrangers en France depuis la mise en œuvre du traitement AGDREF.

Le ministère de l'Intérieur souhaite en premier lieu utiliser le Fichier AGDREF pour assurer la gestion des demandes de titre d'identité républicain et de document de circulation pour étranger mineur et l'édition de ces documents.

Ces titres, institués postérieurement à la mise en œuvre du fichier AGDREF, sont destinés aux étrangers qui, du fait de leur minorité, ne peuvent se voir délivrer une carte de séjour. Ils permettent d'attester de la régularité du séjour de l'étranger mineur et de lui permettre, lorsqu'il quitte le territoire national, d'y être réadmis sur présentation de ce titre.

Le ministère de l'Intérieur souhaite, en deuxième lieu, intégrer au fichier AGDREF une application de traitement de texte permettant à son service des étrangers de gérer les nombreux courriers qu'elle reçoit, de consulter le fichier AGDREF afin d'y répondre et d'éditer la réponse apportée à la requête.

Cette modification permettra également d'informatiser, sous forme d'index, les dossiers sur support papier que ce service a créés chaque fois qu'il a reçu un courrier.

Le ministère de l'Intérieur souhaite enfin profiter de cette modification pour prendre en compte la possibilité nouvelle de délivrance des titres de séjour sous la forme d'étiquette autocollante à apposer sur le passeport.

La Commission observe que l'intégration de ces nouvelles fonctionnalités n'implique aucune modification de la liste des informations nominatives collectées et traitées, telle qu'elle résulte de l'article 2 du décret du 29 mars 1993.

Elle prend également note que les durées de conservation arrêtées sont identiques à celles qui avaient été fixées lors de la déclaration initiale de cette application.

S'agissant des destinataires des informations nominatives collectées et traitées, le ministère de l'Intérieur a souhaité, à côté des organismes sociaux, pouvoir transmettre les informations statistiques issues du fichier AGDREF à l'INSEE et à l'INED, à leur demande et après les avoir rendues totalement anonymes.

Émet un avis favorable concernant le projet de décret modificatif portant création d'AGDREF présenté par le ministère de l'Intérieur, ainsi que le projet d'acte réglementaire présenté par la CNAF, sous réserve que :
— le fichier « réponse » transmis par le ministère de l'Intérieur précise, en cas de présence d'un code « purgé » ou « archivé », le motif de la purge ou de l'archivage ;
— le projet d'acte réglementaire de la CNAF soit modifié de façon à prévoir que la personne faisant l'objet d'un contrôle soit informée du résultat des rapprochements des informations et mise en mesure de faire valoir ses observations avant toute prise de décision la concernant.

Exprime *sa* grave préoccupation s'agissant de la mise à jour et de l'apurement du fichier AGDREF, qui doivent être réalisés régulièrement, ainsi que la Commission l'avait demandé dans sa délibération du 7 mai 1991, et **souhaite être informée** des mesures prises à cet effet par le ministère de l'Intérieur.

Demande que :
— un dispositif de chiffrement pour les transmissions d'informations entre le CSN et le centre informatique du ministère de l'Intérieur soit mis en œuvre dans un délai d'un an afin d'assurer la confidentialité des données échangées ;
— un bilan relatif à la mise en œuvre de la nouvelle procédure automatisée d'interro gation du fichier AGDREF soit adressé à la Commission par la CNAF après une année de mise en œuvre effective.

Délibération n° 02-067 du 24 septembre 2002 portant avis sur la mise en oeuvre, par la Croix-Rouge française, d'un traitement d'informations nominatives dont l'objet est d'assurer la délivrance de badges d'accès aux personnes hébergées dans le centre d'accueil de Sangatte

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par la Croix-Rouge française, en application de l'article 15 de la loi du 6 janvier 1978 d'un projet de décision du conseil d'administration portant création d'un traitement d'informations nominatives dont l'objet est d'assurer la délivrance de badges d'accès aux personnes hébergées dans le centre d'accueil de Sangatte ;

Vu le préambule de la Constitution du *17* octobre 1946 ;

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

Vu la directive n° 95/46/CE du Parlement européen et du conseil du 24 octobre 1998 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données ;

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

Vu la loi n° 52-893 du 25 juillet 1952 modifiée relative au droit d'asile pris ensemble le décret n° 98-503 du 23 juin 1998 pris pour l'application de la loi n° 52893 relative au droit d'asile et relatif à l'asile territorial ;

Vu le projet de décision du conseil d'administration de la Croix-Rouge française ;

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

La Croix-Rouge française a saisi la CNIL d'une demande d'avis portant sur la mise en œuvre d'un traitement d'informations nominatives dont la finalité est de permettre la délivrance de badges d'accès aux personnes hébergées dans le centre d'accueil de Sangatte afin de leur assurer une plus grande sécurité au sein du centre et de permettre une meilleure gestion des prestations qui leur sont fournies ;

Ce centre d'accueil d'urgence, créé en 1999 par arrêté préfectoral, a pour mission d'assurer l'hébergement, à titre transitoire, de ressortissants étrangers, selon les modalités définies par la convention conclue à cet effet entre l'État et la Croix-Rouge ; dans le cadre de cette mission humanitaire, la Croix-Rouge est ainsi chargée de fournir à ces personnes, non seulement l'hébergement mais également les repas, les premiers soins ainsi que des mesures d'accompagnement social et administratif.

Le dispositif proposé consiste à délivrer à l'ensemble des personnes accueillies dans le centre un badge d'accès comportant la photographie de l'intéressé ; ce badge devra être présenté pour pouvoir accéder au centre et bénéficier des prestations servies. Il devra être restitué au centre lors de chaque sortie, à charge pour le résident lorsqu'il se représentera à l'entrée du centre, de le redemander en communiquant le numéro du badge ou en déclinant l'identité qu'il avait précédemment déclarée.

L'établissement des badges nécessite la création d'un fichier qui, tenu sous la responsabilité de la Croix-Rouge avec l'aide d'un prestataire technique, permettra de vérifier, à chaque entrée, qu'il s'agit bien d'un résident du centre. Dans la perspective de la fermeture du centre et des démarches d'accompagnement social et administratif qui seront engagées en faveur des personnes hébergées, ce fichier pourra également être consulté lors de l'examen de chaque situation.

La Commission considère que, eu égard à la précarité de la situation des personnes hébergées et à la sensibilité des informations recueillies, la mise en oeuvre de ce fichier doit être entourée de garanties particulières, de nature à assurer à ces personnes la nécessaire confidentialité des informations les concernant.

La Commission relève ainsi que seuls les agents concernés de la Croix-Rouge ainsi que, sous leur contrôle, les personnels désignés du prestataire technique appelés à gérer l'application, auront accès au fichier. Il importe que ces agents et personnels soient dûment habilités par le directeur du centre.

Dans le cadre de leur mission humanitaire, les experts du haut commissariat aux Réfugiés pourront ponctuellement, en tant que de besoin, consulter sur place des informations issues de ce fichier.

La Commission estime que cet accès est légitime et que l'acte réglementaire portant création du traitement doit en faire mention.

Elle prend acte qu'il ne sera procédé à aucune transmission d'informations.

Le fichier enregistrera les informations suivantes, telles que déclarées par l'intéressé, et sans qu'il soit procédé à une vérification des identités : les noms, prénoms et alias, la date de naissance, le sexe, la nationalité, la photographie, le lien de parenté pour les mineurs accompagnés, ainsi que le cas échéant, l'indication « mineurs isolés », le numéro d'ordre au badge, la date de la demande et éventuellement celle du renouvellement.

Sur le badge, ne figureront que les noms et prénoms, l'année de naissance, la nationalité ainsi qu'une photographie d'identité et un numéro d'ordre.

La nationalité sera recueillie pour permettre aux services de la Croix-Rouge d'assurer une répartition adéquate des places d'hébergement, préparer la constitution des dossiers administratifs des personnes accueillies et disposer d'états statistiques. Cette information est appelée à figurer également sur le badge, pour faciliter la tâche des traducteurs présents sur le site.

La Commission estime que le recueil de ces informations est pertinent au regard des objectifs poursuivis.

Le traitement sera mis en oeuvre sur des moyens informatiques situés dans les locaux du centre et exploités par des agents déjà société prestataire de services, sous le contrôle des services de la Croix-Rouge. À cet effet le contrat passé entre la Croix-Rouge et ce prestataire comporte une clause de sécurité par laquelle ce dernier s'engage à respecter la confidentialité des informations auxquelles il aura accès. Le fichier sera protégé par une procédure de mots de passe individuels, des mesures de sécurité physique rigoureuses (surveillance des locaux) étant par ailleurs adoptées.

Il est prévu que les données enregistrées soient conservées jusqu'à la fermeture effective du centre.

La Commission prend acte de ce que les personnes accueillies dans le centre seront informées, selon des modalités adaptées (par le soin des traducteurs présents sur le site et par des mentions sur le formulaire de demande de badge), des finalités de ce recueil d'informations, des destinataires, des modalités d'utilisation des badges et des conditions d'exercice de leur droit d'accès.

Émet, compte tenu des garanties apportées, **un avis favorable** à la mise en œuvre, par la Croix-Rouge, du traitement d'informations nominatives ayant pour objet d'assurer la délivrance de badges aux personnes hébergées dans le centre de Sangatte, sous réserve que l'article 3 de l'acte réglementaire portant création du traitement soit complété de façon à indiquer d'une part, que seuls les agents de la Croix-Rouge et les personnes agissant pour son compte, dûment habilités par le directeur du centre, seront destinataires de l'ensemble des informations, d'autre part, que les experts du haut commissariat aux Réfugiés pourront ponctuellement, en tant que de besoin, consulter sur place des informations issues de ce fichier.

Délibération n° 02-094 du 10 décembre 2002 concernant un projet de décret modifiant le décret n° 97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministre des Affaires sociales, du Travail et de la Solidarité et le ministre de la Santé, de la Famille et des Personnes handicapées d'un projet de décret modifiant le décret n° 97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et, pris 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 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° 97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie ;

Vu le décret n° 98-275 du 9 avril 1998 relatif à la carte d'assurance maladie et modifiant le Code de la Sécurité sociale ;

Vu le projet de décret présenté par le ministre des affaires sociales, du travail et de la solidarité et le ministre de la santé, de la famille et des personnes handicapées ;

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

Formule les observations suivantes :

Le projet de décret dont est saisie la Commission a principalement pour objet d'adapter le dispositif SESAM Vitale aux pratiques de certaines catégories des professionnels de santé et à certaines difficultés qui sont apparues lors de la mise en place du système.

Ce texte tend, en particulier, à aménager le mode de signature des feuilles de soins électroniques de façon à résoudre certains problèmes rencontrés par les professionnels de santé libéraux dès lors que la feuille de soins électronique ne peut être établie en présence de l'assuré ou lorsqu'il existe un décalage dans le temps entre l'établissement de la feuille de soins et la réalisation de l'acte ou de la prestation.

En conséquence, l'article 2 du projet de décret conserve le principe de la signature conjointe de l'assuré et du professionnel de santé sur la feuille de soins, mais ne prévoit plus l'exigence d'une lecture simultanée de la carte de professionnel de santé et de la carte Vitale de l'assuré.

La Commission estime que la désynchronisation des signatures doit être limitée à des situations particulières tenant compte des contraintes de gestion propres à certains modes d'exercices professionnels et que le principe de la lecture simultanée des cartes doit demeurer la règle.

La Commission prend également acte qu'aux termes de l'article 2 -2°, un procédé technique garantira le maintien de l'intégrité des données constitutives de la feuille de soins jusqu'à transmission de celle-ci aux fins de remboursement, cela dès l'obtention de la signature du bénéficiaire. L'instauration d'un tel dispositif est de nature à satisfaire aux obligations de sécurités définies à l'article 29 de la loi du 6 janvier 1978 et notamment à empêcher la déformation des données.

L'article 3 a pour objet de permettre aux professionnels de santé intervenant en clinique privée de mandater un « tiers de confiance » (un confrère ayant une qualification équivalente, le directeur de l'établissement ou son représentant) pour signer les éléments de facturation correspondant à leurs honoraires.

La Commission prend acte qu'aux termes de l'article 3 -2°, la facturation des frais présentés au remboursement sera établie sous la responsabilité exclusive du professionnel de santé auteur de l'acte, tant en ce qui concerne l'attestation de la réalisation de celui-ci que sa cotation, à partir des éléments certifiés par lui.

Cette procédure est de nature à permettre aux professionnels de santé de s'assurer de l'exactitude des informations relatives à leurs actes et prestations.

L'article 6 du projet de décret prévoit que lorsque les feuilles de soins électroniques sont transmises à l'assurance maladie par l'intermédiaire d'organismes concentrateurs techniques ceux-ci doivent être agréés dans des conditions fixées par arrêté pris après avis de la CNIL.

L'introduction de cette disposition est conforme aux recommandations de la Commission sur la nécessité d'un encadrement juridique de l'activité de ces organismes.

Enfin, le projet de décret comporte plusieurs dispositions tendant à permettre une simplification et une amélioration de la gestion du dispositif tant pour les caisses d'assurance maladie que pour les professionnels et les usagers du système de soins.

Est d'avis que le projet de décret modifiant le décret n° 97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie soumis par le ministre des Affaires sociales, du Travail et de la Solidarité et par le ministre de la Santé, de la Famille et des Personnes handicapées n'appelle pas d'observations particulières au regard des dispositions de la loi du 6 janvier 1978.

Spoliations

Délibération n° 02-055 du 9 juillet 2002 relative à un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part l'instruction des dossiers d'information présentés en application du décret n° 99-778 du 10 septembre 1999 modifié, d'autre part le paiement des indemnisations servies sur la base du présent décret

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le Premier ministre d'un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer, d'une part l'instruction des dossiers d'indemnisation présentés en application du décret n° 99-778 du 10 septembre 1999, modifié, instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation et, d'autre part, le paiement des indemnisations servies sur la base du présent décret ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 31 ;

Vu le décret n° 99-778 du 10 septembre 1999 instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation modifié par les décrets n° 2000-932 du 25 septembre 2000 et 2001-530 du 20 juin 2001 ;

Vu le décret 2000-1023 du 19 octobre 2000 portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 au fichier mis en œuvre par la commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation ;

Après avoir entendu monsieur Maurice Benassayag, commissaire en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement en ses observations ;

Observe :

La Commission a été saisie par le Premier ministre d'un projet de décret portant création de deux traitements automatisés d'informations nominatives pour assurer, d'une part l'instruction des dossiers d'indemnisation présentés en application du décret n° 99-778 du 10 septembre 1999, modifié, instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation et, d'autre part, le paiement des indemnisations servies sur la base du présent décret.

Aux termes du décret susvisé, la commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant

l'Occupation (CIVS) est chargée de rechercher et de proposer les mesures de réparation, de restitution ou d'indemnisation appropriées. Lorsque la CIVS propose que l'État prenne à sa charge une mesure d'indemnisation, elle transmet sa recommandation au Premier ministre (secrétariat général du gouvernement — SGG). Les décisions d'indemnisation prises par le Premier ministre sur la base des recommandations de la commission sont notifiées aux intéressés et à l'Office national des anciens combattants et victimes de guerre (ONACV) qui est chargé de les exécuter.

Le premier traitement automatisé, qui sera mis en œuvre par la direction des services administratifs et financiers (DSAF) du Premier ministre, permettra d'assurer l'instruction des dossiers d'indemnisation. Le second traitement, qui sera mis en œuvre par l'office national des anciens combattants et victimes de guerre, permettra d'assurer le paiement des indemnités accordées.

Ces traitements, en ce qu'ils prévoient l'enregistrement d'informations concernant des personnes demandant à bénéficier de la mesure de réparation prévue par le décret du 10 septembre 1999, un projet de décret portant application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 aux fichiers mis en œuvre pour l'application de ce décret est soumis à l'avis de la Commission.

/ — Sur le traitement automatisé d'informations nominatives ayant pour finalité l'instruction des dossiers d'indemnisation

Ce traitement sera mis en œuvre par la cellule d'indemnisation du bureau des affaires juridiques et contentieuses au sein de la direction des services administratifs et financiers (DSAF) du Premier ministre qui est chargé, aux termes du décret du 10 septembre 1999, de prendre les décisions d'indemnisation sur la base des recommandations de la commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation.

Les informations enregistrées seront les nom et prénom du demandeur, date de naissance du demandeur, adresse du demandeur, nom du rapporteur, date de séance et d'avis de la commission, observations résumées du commissaire du Gouvernement, le cas échéant, décision prise par le Premier ministre, montant de l'indemnisation.

Les destinataires des données seront les agents du secrétariat général du Gouvernement et les agents de l'Office national des anciens combattants et victimes de guerre, chargés d'assurer le traitement des dossiers d'indemnisations liés à l'application du décret du 10 septembre 1999 susvisé. Ces agents seront habilités nominativement par arrêté du Premier ministre.

Les informations seront détruites à l'expiration d'un délai de trois ans. Le droit d'accès et de rectification s'exercera auprès du secrétariat général du gouvernement.

// — Sur le traitement automatisé d'informations nominatives ayant pour finalité le paiement des mesures de réparation

Ce traitement sera mis en œuvre par l'Office national des anciens combattants et victimes de guerre (l'ONACVG), établissement public placé sous la tutelle du ministre de la défense, chargé, aux termes du décret du 10 septembre 1999, d'assurer l'exécution des décisions d'indemnisation prises par le Premier ministre.

Les informations enregistrées dans le traitement automatisé seront celles relatives au nom et prénoms du demandeur, date de naissance du demandeur, adresse du demandeur, décision prise par le Premier ministre, les numéros des décisions du Premier ministre, les coordonnées bancaires ou postales des bénéficiaires, les numé-

ros de dossiers attribués par l'Office, les montants versés, la devise de règlement et les dates de versement se rapportant aux dossiers ayant fait l'objet d'une décision positive du Premier ministre et transmises à l'ONACVG par le SGG.

Les destinataires des données seront les agents de l'Office national des anciens combattants et victimes de guerre chargés d'assurer le paiement des indemnisations servies en application du décret du 10 septembre 1999 susvisé.

Les données faisant l'objet du traitement seront détruites à l'expiration d'un délai de quatre ans à compter de la date de paiement de l'indemnisation.

Le droit d'accès et de rectification s'exercera auprès du directeur général de l'Office national des anciens combattants et victimes de guerre.

Au bénéfice de ces observations, émet un avis favorable sur le projet de décret dont elle a été saisie par le Premier ministre.

Délibération n° 02-056 du 9 juillet 2002 relative à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 aux fichiers mis en œuvre pour l'application de décret du 10 septembre 1999 modifié instituant une commission pour l'indemnisation des victimes en spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le Premier ministre d'un projet de décret pris en application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers mis en œuvre pour l'application du décret du 10 septembre 1999 modifié instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et notamment son article 31 ;

Vu le décret n° 99-778 du 10 septembre 1999 instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation modifié par les décrets n° 2000-932 du 25 septembre 2000 et 2001-530 du 20 juin 2001 ;

Vu le décret 2000-1023 du 19 octobre 2000 portant application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 au fichier mis en œuvre par la commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation ;

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

Formule les observations suivantes :

La Commission est saisie par le Premier ministre d'un projet de décret portant création de deux traitements automatisés d'informations nominatives visant à assurer, pour l'un l'instruction des dossiers d'indemnisation des victimes de spoliations telles que définies par les dispositions du décret n° 99-778 du 10 septembre 1999 modifié instituant une commission pour l'indemnisation des victimes de spoliations intervenues du fait des législations antisémites en vigueur pendant l'occupation, pour l'autre la mise en paiement des indemnités servies sur la base de ce décret.

Ces deux traitements devant comporter des informations nominatives relatives aux personnes qui, remplissant les conditions prévues par le décret du 10 septembre 1999 modifié, demanderont à être indemnisées du préjudice subi par elles-mêmes ou par leurs ascendants du fait des législations antisémites pendant l'Occupation, les fichiers envisagés relèveront des dispositions de l'article 31 de la loi du 6 janvier 1978.

Aux termes de l'article 31 de la loi, la collecte et le traitement des informations nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs des personnes sont interdites sauf accord exprès de l'intéressé, à moins qu'il ne soit fait exception à cette interdiction pour des motifs d'intérêt public, par décret en Conseil d'État pris sur proposition ou avis conforme de la Commission.

Au cas d'espèce, la Commission estime que l'objectif poursuivi par le gouvernement, qui est de procéder à l'indemnisation des victimes ou des ayants droit des victimes de spoliations du fait des législations antisémites en vigueur durant l'Occupation, constitue un motif d'intérêt public justifiant l'application de la dérogation prévue par l'article 31 de la loi du 6 janvier 1978 aux deux traitements automatisés d'informations nominatives nécessaires à la gestion des droits des intéressés.

Compte tenu de ces observations, la Commission :

Émet un avis conforme au projet de décret tel qu'il a été soumis par le Premier ministre sous réserve que ce texte vise le décret portant création des deux traitements mis en œuvre.

Statistiques

Délibération n° 02-002 du 24 janvier 2002 concernant un traitement automatisé de l'INSEE visant à l'exploitation d'informations fiscales pour l'élaboration et la diffusion de produits statistiques locaux sur les revenus des ménages, l'impôt sur le revenu et la taxe d'habitation relative à la résidence principale

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Economie, des Finances et de l'Industrie d'un projet d'arrêté « portant autorisation d'un traitement automatisé d'informations nominatives visant à l'exploitation de données fiscales pour l'élaboration et la diffusion de produits statistiques locaux sur les revenus des ménages, l'impôt sur le revenu et la taxe d'habitation relative à la résidence principale » ;

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

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

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

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

Vu l'arrêté du 5 janvier 1990 modifiant l'arrêté relatif au traitement informatisé d'impôt sur le revenu à la direction générale des impôts, notamment son article 6 ;

Vu l'arrêté du 8 mars 1996 régissant le traitement informatisé de la taxe d'habitation à la direction générale des impôts, notamment son article 5 ;

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

Rend l'avis suivant :

Le ministère de l'Economie, des Finances et de l'Industrie a saisi la Commission d'une demande d'avis portant sur un traitement automatisé mis en place par l'INSEE pour assurer la diffusion de produits statistiques locaux obtenus à partir de l'exploitation des fichiers des déclarations de revenu global des personnes physiques et de gestion de la taxe d'habitation. Ces fichiers lui sont transmis chaque année par la Direction générale des impôts (DGI) sur support informatique, dans les conditions définies par l'article 7 bis de la loi du 7 juin 1951 et conformément aux arrêtés des 5 janvier 1990 et 8 mars 1996 susvisés.

Ces produits statistiques (indicateurs de répartition, moyennes, tableaux de variables croisées, fichiers-détail) ont pour objet principal de décrire, pour des zones géographiques prédéfinies ou non par l'INSEE, les niveaux et disparités de revenus bruts et des impôts de base des ménages — l'impôt sur le revenu et la taxe d'habitation liée à la résidence principale.

Sur les informations utilisées par l'INSEE

Les fichiers de l'administration fiscale qui sont utilisés pour la confection des résultats statistiques sont :

— le fichier de l'ensemble des déclarations fiscales de revenus reçues par la DGI pour une année donnée (« POTE ») qui, utilisé seul, permet d'analyser les informations déclarées par foyer fiscal ou par personne ;

— le fichier de gestion de la taxe d'habitation (« FLFC ») qui sert notamment au rapprochement des foyers fiscaux répertoriés dans un même logement taxé en résidence principale qui constituent, de ce fait, un même ménage au sens statistique.

Les conditions générales d'exploitation par l'INSEE de ces informations et celles de la production et de la diffusion des données statistiques issues de leur traitement font l'objet de « protocoles d'accord » co-signés par les deux administrations.

Sur les modalités de traitement des informations reçues de l'administration fiscale

Une base nationale de données relatives aux ménages, aux revenus et aux impôts précités est créée. Elle regroupe par ménage les seules informations issues des fichiers de la DGI qui sont nécessaires à la production des résultats statistiques envisagés, jusqu'à ce que leur archivage soit décidé. Ces informations revêtent un caractère indirectement nominatif du fait de la présence, en leur sein, de codes géographiques particulièrement fins (code îlot INSEE, code commune, qu'elle qu'en soit la taille). En conséquence, l'INSEE a prévu d'adopter, pour la gestion de la base de données nationale, des mesures de sécurité renforcées.

La mise à jour de la base nationale donne, par ailleurs, lieu à la constitution de fichiers de travail qui sont conservés le temps nécessaire à la réalisation des opérations de regroupement des fichiers « POTE et FLFC » et de vérification des résultats ainsi obtenus. Ce délai a été fixé à six mois. Il est cependant prévu de conserver, par dérogation, l'ensemble des fichiers de travail pendant les trois années de la phase de mise au point du dispositif.

Seuls les agents de l'INSEE disposant d'une habilitation spéciale sont destinataires des informations contenues dans la base nationale ou dans les fichiers de travail ou peuvent y avoir accès.

Par ailleurs, les produits statistiques destinés à être diffusés qui, par hypothèse, sont anonymisés, sont conservés dans des bases de diffusion qui sont susceptibles d'être mises à la disposition des directions régionales de l'INSEE. Ces produits qui ont vocation à être publiés et communiqués à toute personne intéressée dans les conditions fixées par l'arrêté, sont mis à la disposition des utilisateurs potentiels sous des formes et sur des supports adaptés à leurs besoins.

La Commission prend acte de ces modalités de traitement interne des informations fiscales par l'INSEE qui paraissent satisfaisantes.

Sur *les conditions de la diffusion au public des produits statistiques*

Les produits statistiques sont mis à la disposition des publics intéressés à des niveaux géographiques définis en fonction de leur degré de précision et selon des modalités tenant compte de leur nature. Ainsi, certains indicateurs, fichiers et tableaux sont destinés au seul public institutionnel ou supposent, pour être communiqués, la signature d'une licence d'usage.

S'agissant de données principalement quantitatives (montants de revenus et d'impôts), l'INSEE privilégie la communication d'indicateurs de distribution non additifs, qui portent autant sur l'évaluation des revenus et des impôts des ménages composant la population d'une zone géographique que sur leur répartition au sein

de cette population. Ces indicateurs donnent, en effet, une meilleure perception de la réalité socio-économique d'une zone et de la disparité des situations individuelles que les seuls montants du revenu fiscal moyen et des cotisations moyennes des impôts, qui accordent une place excessive aux valeurs extrêmes. Ainsi, ces indicateurs sont de nature à assurer une meilleure protection de la confidentialité des données personnelles, en ne donnant que des niveaux de revenus au-dessous — ou au-dessus (pour les dernières tranches) — desquels se trouve une fraction de la population.

Enfin, le caractère non-additif de ces indicateurs signifie qu'il est techniquement impossible de déduire, à partir des informations relatives à deux zones dont l'une recouvre l'autre, des renseignements sur la zone obtenue par recoupement. En conséquence, leur diffusion peut s'affranchir de la contrainte de non-recoupement des zones qui est primordial pour le respect des seuils de diffusion choisis dans le cas des indicateurs additifs (moyennes, simples comptages...). De même, la contrainte de continuité des zones, selon laquelle les indicateurs ne doivent porter que sur des zones d'un seul tenant, n'est pas pertinente pour les indicateurs non additifs.

L'INSEE propose, aux articles 3 et 4 du projet d'arrêté, que soient communicables au « public général » comme au « public sous licence » un certain nombre d'indicateurs :

— Au niveau d'un îlot, d'une commune ou de tout regroupement de ces enti tés, à la condition expresse que la zone choisie rassemble un minimum incompres sible de cinquante ménages :
1) les dénombrements simples des ménages, des personnes et des unités de consommation de la zone ;
2) les médianes de la distribution du revenu fiscal — avant prise en compte des abattements — calculées pour l'ensemble des ménages, des personnes ou des unités de consommation.

— Pour des zones correspondant aux IRIS 2000, à des communes d'au moins 2 000 habitants ou à tout regroupement institutionnel de communes (établisse ments publics intercommunaux, pays, cantons...), des indicateurs se rapportant à la population globale de la zone :
1) les quartiles et déciles de la distribution du revenu fiscal, pour les ménages, les personnes et les unités de consommation (indicateurs non additifs) ;
2) les écarts-type et les indices de Gini de la distribution du revenu fiscal dans l'ensemble des ménages, des personnes et des unités de consommation (indicateurs non additifs) ;
3) les parts respectives de certaines catégories de revenus au sein du revenu fiscal global : salaires et indemnités journalières et de chômage ; bénéfices nets des profes sions non salariées ; pensions, retraites et rentes viagères ; autres revenus fiscaux (indicateurs non additifs) ;
4) le revenu fiscal moyen par ménage, par personne et par unité de consommation ;
5) la proportion des ménages imposés.

— Pour des zones correspondant au regroupement de trois IRIS 2000, à des communes ou à des regroupements de communes, à la condition que leur population atteigne au moins 5 000 habitants, quelques indicateurs concernant les seuls ména ges imposables :
1) les quartiles de la taxe d'habitation et de l'impôt sur le revenu (indicateurs non additifs) ;
2) les montant moyens de l'impôt sur le revenu et de la taxe d'habitation par ménage, par personne et par unité de consommation.

Les indicateurs non additifs, identifiés comme tels ci-dessus, pourront, en outre, être communiqués pour toute zone, d'un seul tenant ou non, définies par l'utilisateur à partir de communes et d'îlots, dans le respect des mêmes seuils de population minimale.

Les mêmes indicateurs, lorsqu'ils se rapportent à la population globale de la zone, pourront être calculés pour des sous-populations particulières, définies par l'utilisateur à l'aide des critères socio-démographiques présents dans les fichiers de la DGI — ce qui a pour effet d'exclure tout critère sensible — (ex. : le sexe et l'âge de la personne de référence du ménage, la taille du ménage, la nature des revenus perçus), sous les conditions suivantes :

— la population totale de la zone considérée devra être au moins de l'ordre de 10 000 habitants ;

— chaque sous-population étudiée devra représenter au niveau national, sur la base de la source fiscale traitée, au moins 1/10^{e} de la population totale ;

— les zones de diffusion demandées par un même client ne devront pas se recouper pour une année donnée et l'INSEE tiendra, pour s'assurer de l'absence de recoupe ment, un registre national des bénéficiaires de ces fichiers.

Le seuil de 10 000 habitants sera également appliqué pour la diffusion :

— des déciles de distribution de deux catégories spécifiques de revenus : les salai res ; les pensions, retraites et rentes viagères ;

— du nombre total de ménages, de personnes et d'unités de consommation chaque fois concernés ;

— des déciles de la distribution de l'impôt sur le revenu pour les seuls ménages, per sonnes et unités de consommation imposés.

Par ailleurs, l'article 6 du projet d'arrêté prévoit que les collectivités locales, administrations et établissements publics ayant une mission de création ou de gestion de service public pourront, après signature d'une licence d'usage avec l'INSEE, obtenir communication des quartiles et des proportions de certaines sources de revenus au sein du revenu fiscal global — normalement diffusés au niveau minimal des IRIS 2000 et des communes d'au moins 2 000 habitants — au niveau plus fin de l'îlot, de la commune ou de tout regroupement, à la condition que ces zones comportent un minimum de cinquante ménages et sous réserve de la signature d'une licence d'usage.

En ce qui concerne la diffusion de tableaux, l'article 5 du projet en fixe ainsi les limites : ceux-ci sont exclusivement destinés à décompter, pour des zones pré-établies par l'INSEE, les ménages, personnes et unités de consommation en fonction non pas des revenus qu'ils perçoivent ou des impôts qu'ils versent, mais de certaines variables socio-démographiques, toutes issues des fichiers de l'administration fiscale : le type de ménage, le sexe et l'âge de la personne de référence, le nombre de personnes à charge par âge, le nombre de personnes par ménage ayant bénéficié de revenus d'activité (sans distinguer entre les périodes d'emploi et de chômage), le nombre de personnes ayant bénéficié de retraites ou pensions par ménage.

Les règles de communication de ces tableaux s'inspirent, lorsque cela est possible, des modalités retenues pour les informations provenant du recensement de la population :

— pour le « public sous licence » : au niveau de l'îlot ou de la commune ;

— pour le « public général » : au niveau de l'IRIS 2000, de la commune, du canton ou de l'arrondissement.

Cependant, les tableaux utilisant les variables « nombre de personnes à charge » et « nombre de personnes ayant bénéficié de certaines catégories de reve-

nus par ménage » ne pourront être diffusés au « public général » qu'au niveau des IRIS 2000 ou de zones d'au moins 2 000 habitants, afin de se prémunir contre toute divulgation de la situation fiscale déclarée par les ménages.

Enfin, des fichiers-détail non nominatifs, constitués par ménage pourront être communiqués dans le respect des précautions suivantes :

1) ils ne seront disponibles que pour des zones — qu'elles soient prédéfinies ou spécialement constituées à la demande de l'utilisateur — représentant une population d'au moins 100 000 habitants ;

2) leur communication supposera la signature d'une licence d'usage ;

3) un même client ne pourra pas demander ces fichiers, pour une année donnée, pour des zones de diffusion se recoupant, et l'INSEE tiendra un registre national des bénéficiaires de fichiers-détail afin de s'assurer de l'application de cette condition.

La Commission estime que le dispositif d'ensemble retenu pour la cession des produits statistiques locaux répond à son souhait d'éviter tout risque d'identification de personnes physiques concernées par une situation fiscale précise.

La Commission rappelle cependant que, s'agissant de résultats obtenus à partir du traitement d'informations provenant de la DGI, les modalités d'exploitation de ces dernières doivent, préalablement à leur entrée en vigueur, avoir été acceptées par l'administration fiscale, ce qui devrait se traduire par une modification du « protocole d'accord » concernant la communication annuelle d'informations relatives à l'impôt sur le revenu des personnes physiques et à la taxe d'habitation, signé en 2000 par l'INSEE et la DGI.

Au bénéfice de ces observations, la Commission émet un avis favorable sur le projet d'arrêté qui lui est soumis par le ministère de l'Économie, des Finances et de l'Industrie.

Délibération n° 02-009 du 7 mars 2002 relative au projet de décret en Conseil d'État portant extension en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, dans les terres australes et antarctiques françaises et à Mayotte du décret n° 78-774 du 17 juillet 1978

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministère de la Justice d'un projet de décret en Conseil d'Etat portant extension aux territoires d'outre-mer (Polynésie française, terres australes et antarctiques françaises, îles de Wallis et Futuna), à la Nouvelle-Calédonie et à la collectivité départementale de Mayotte du décret n° 78-774 d'application de la loi du 6 janvier 1978 ;

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

Vu la 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 ;

Après avoir entendu Monsieur Gérard Gouzes, commissaire, en son rapport et Madame Charlotte-Marie Pitrat, commissaire du gouvernement, en ses observations ;

La Commission prend acte de l'extension aux territoires d'outre-mer (Polynésie française, terres australes et antarctiques françaises, îles de Wallis et Futuna), à la Nouvelle-Calédonie et à la collectivité départementale de Mayotte du décret n° 78-774 du 17 juillet 1978, portant application de la loi du 6 janvier 1978.

Elle observe que les seules dispositions du décret du 17 juillet 1978 qui ne sont pas étendues à ces territoires et collectivités concernent les dispositions d'application du chapitre V ter de la loi du 6 janvier 1978 et de l'article L. 288 du Livre des procédures fiscales dont l'extension à ces territoires et collectivités n'a pas été prévue par la loi.

Compte tenu de ces observations, **émet un avis favorable** au projet de décret portant extension en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, dans les terres australes et antarctiques françaises et à Mayotte du décret n° 78-774 du 17 juillet 1978.

Délibération n° 02-011 du 7 mars 2002 portant avis sur un projet de décret portant application de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'enregistrement et à la conservation d'informations relatives aux actes de l'état civil par les mairies de la collectivité départementale de Mayotte, par le greffe du tribunal de première instance de Mamoudzou, par le secrétariat d'Etat à l'outre-mer ainsi que par la Commission de révision de l'état civil chargée d'établir les actes qui auraient dû être portés sur les registres de l'état civil de droit commun et de droit local de Mayotte

La Commission nationale de l'informatique et des libertés ;

Saisie par la ministre de la Justice d'un projet de décret en Conseil d'Etat portant application de l'article 31 de la loi du 6 janvier 1978 ;

Vu l'article *75* de la Constitution ;

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

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

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

Vu l'ordonnance n° 2000-218 du 8 mars 2000 fixant les règles de détermination des nom et prénom des personnes de statut civil de droit local applicables à Mayotte ;

Vu l'ordonnance n° 2000-219 du 8 mars 2000 relative à l'état civil à Mayotte ;

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

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

Formule les observations suivantes :

Les dispositions relatives à l'état civil à Mayotte, telles que fixées par les ordonnances susvisées du 8 mars 2000 et celles relatives à la dualité de statut, consacrée par l'article 75 de la Constitution, font obligation tant aux officiers de l'état civil qu'à la commission de révision de l'état civil, instituée par l'ordonnance n° 2000-218 du 8 mars 2000, d'inscrire les actes concernant une personne relevant du statut civil de droit local applicable à Mayotte et de transcrire les mentions relatives à sa situation maritale, renseignant ainsi sur son état ou non de polygamie.

Les mentions qui sont ainsi portées sur les actes de l'état civil à Mayotte doivent être considérées comme faisant apparaître, directement ou indirectement, l'origine raciale des personnes, leurs opinions religieuses ainsi que leurs mœurs, pour ce qui concerne les mentions relatives à l'état de polygamie.

La Commission est saisie d'un projet de décret tendant à autoriser, conformément à l'article 31 de la loi du 6 janvier 1978, l'enregistrement dans les registres d'état civil, de ces informations.

La Commission estime que la collecte de ces informations, compte tenu du régime juridique propre à la collectivité départementale de Mayotte, répond à un motif d'intérêt public, au sens de l'alinéa 3 de l'article 31.

Émet en conséquence un avis conforme au projet de décret portant application des dispositions de l'article 31 de la loi du 6 janvier 1978, sous réserve que l'article 1er soit rédigé ainsi : *« les mairies de Mayotte, le greffe du tribunal de première instance de Mamoudzou, le service de l'état civil du secrétariat d'État à l'outre-mer, pour les besoins de la tenue des registres de l'état civil de droit commun et de droit local applicable à Mayotte, ainsi que la commission de révision de l'état civil instituée par l'article 18 de l'ordonnance n° 2000-218 du 8 mars 2000 précitée, pour les besoins de la gestion des dossiers relatifs aux demandes tendant à faire établir un des actes prévus à l'article 20 de ladite ordonnance, sont autorisée à enregistrer et conserver les données à caractère personnel relatives à la polygamie et au statut civil des personnes, qui relèvent des données visées par l'article 31 de la loi du 6 janvier 1978 susvisée. »*

Délibération 02-012 du 14 mars 2002 portant avis sur le projet de décret, présenté par le ministère de l'Économie et des Finances/ 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 en 2002

La Commission nationale de l'informatique et des libertés ;

Saisie par le ministre de l'Économie et des Finances d'un projet de décret en conseil d'Etat, portant application des dispositions de l'article 31 de la loi du 6 janvier 1978 au recensement général de la population à Mayotte ;

Vu l'article *75* de la Constitution ;

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

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

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

V u 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 modifié 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 ;

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

Formule les observations suivantes :

Parmi les informations collectées lors du prochain recensement à Mayotte, figurent les données relatives à la polygamie des personnes, qui sont susceptibles de faire apparaître indirectement les opinions religieuses et les mœurs des personnes interrogées.

La Commission estime que la collecte de ces informations, compte tenu des caractéristiques socio-démographiques et du régime juridique propres à la collectivité départementale de Mayotte, répond à un motif d'intérêt public, au sens de l'alinéa 3 de l'article 31.

Émet en conséquence 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 en 2002.

Délibération n° 02-013 du 14 mars 2002 portant avis sur la mise en œuvre, par le ministère de l'Économie et des Finances, du recensement général de la population (RGP) à Mayotte en 2002

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère de l'Economie et des Finances d'un projet d'arrêté portant création d'un traitement automatisé réalisé à l'occasion du recensement général de la population à Mayotte en 2002 ;

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

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

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 79-18 du 3 janvier 1979 sur les archives ; Vu le décret n° 78-774 du 17 juillet 1978 modifié 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 la délibération n° 02-012 du 14 mars 2002 portant avis sur le projet de décret portant application des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 au traitement automatisé d'informations nominatives mis en oeuvre à l'occasion du recensement général de la population à Mayotte ;

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

Formule les observations suivantes :

La Commission est saisie d'une demande d'avis concernant la mise en oeuvre 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 organisé dans la collectivité départementale de Mayotte en 2002.

Le recensement général de la population (RGP) à Mayotte sera effectué entre juillet et septembre 2002, sous la responsabilité de l'Institut national de la statistique et des études économiques (INSEE).

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 ; cette enquête a un caractère obligatoire.

La Commission observe que les modalités de collecte, d'exploitation et de diffusion des données sont analogues à celles qui ont été définies lors du recense-

ment de 1997 et sur lesquelles elle s'est prononcée favorablement par une délibération du 1er avril 1997.

Les données collectées concerneront les personnes physiques, les logements et immeubles bâtis ; 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, le cas échéant, de la polygamie, le niveau ou la nature de la formation, les langues parlées et écrites, les activités professionnelles, les migrations, les conditions de logement et l'équipement en biens.

La Commission estime qu'au regard des finalités poursuivies, ces catégories d'informations sont adéquates, pertinentes et non excessives.

Les destinataires des données seront l'INSEE et la direction des archives de France ; 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.

La Commission prend acte, qu'à l'égal des modalités de diffusion des données définies lors du recensement de 1997, les données statistiques issues du prochain recensement ne pourront être cédées que sous forme de tableaux statistiques ; ainsi, des tableaux détaillés seront disponibles au niveau de la collectivité départementale, de l'île de la Grande Terre comprenant la commune de Mamoudzou et de la Petite Terre ; des tableaux standards pourront être obtenus au niveau des communes et des cantons et des tableaux résumés seront disponibles au niveau des villages.

La Commission prend note également que les tableaux comportant des données relatives à la polygamie et au statut civil ne pourront être disponibles qu'au niveau de la collectivité départementale.

Certains organismes publics énumérés à l'article 9 du projet d'arrêté (les municipalités et syndicats de communes, 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 également 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.

La Commission prend acte des dispositions prises pour assurer la confidentialité des données et la sécurité du traitement.

La Commission relève enfin que le droit d'accès prévu par l'article 34 de la loi du 6 janvier 1978, s'exercera auprès de l'antenne de l'INSEE à Mayotte.

Compte tenu de ces observations, **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° 02-044 du 30 mai 2002 portant avis sur : — un projet de décret en conseil d'état présenté par le ministère de l'Économie, des Finances et de l'Industrie pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'INSEE à utiliser le RNIPP dans le cadre d'études de mortalité réalisées à partir d'échantillons de population ; — la mise en œuvre par l'INSEE d'applications informatiques relatives à des études de mortalité différentielle réalisées à par tir de la création d'échantillons de population issus du recense ment général de 1999 et du fichier des déclarations annuelles des données sociales

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministre de l'Economie, des Finances et de l'Industrie d'un projet de décret en Conseil d'État pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'INSEE à utiliser le RNIPP dans le cadre d'études de mortalité réalisées à partir d'échantillons de population et de la mise en œuvre par l'INSEE d'applications informatiques relatives à des études de mortalité différentielle réalisées à partir de la création d'échantillons de population issus du recensement général de 1999 et du fichier des déclarations annuelles des données sociales ;

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

Vu la directive n° 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 des données ;

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

Vu la loi n°51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

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

Vu le décret n° 82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques ;

Vu l'arrêté du 22 mai 1998 portant création d'un traitement automatisé réalisé à l'occasion de la collecte et de la diffusion des résultats du recensement général de la population de 1999 ;

Vu le projet de décret en Conseil d'État pris en application de l'article 18 de la loi n° 78-17 du 6 janvier 1978 ;

Vu les projets d'arrêtés présentés par le directeur général de l'INSEE portant création des traitements automatisés relatifs à des études de mortalité différentielle réalisées à partir de la création d'échantillons de population issus du recensement général de 1999 et du fichier des déclarations annuelles des données sociales ;

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

Formule les observations suivantes :

Afin de répondre aux besoins d'information sur les variations de mortalité dans la population, l'Institut national de la statistique et des études économiques saisit la CNIL de deux demandes d'avis relatives respectivement à une étude de la mortalité différentielle réalisée à partir de la création d'échantillons de population issus du recensement général de 1999 et à une étude de mortalité différentielle spécifique des salariés réalisée à partir d'un échantillon issu du fichier des déclarations annuelles des données sociales.

En application des dispositions de l'article 18 de la loi du 6 janvier 1978, l'INSEE souhaite, par ailleurs, être autorisé de façon générale à utiliser le répertoire national d'identification des personnes physiques dans le cadre d'études sur la mortalité réalisées à partir d'échantillons de population afin de connaître le statut vital des personnes de l'échantillon et, le cas échéant, la date de leur décès éventuel.

La Commission prend acte des modalités de consultation du RNIPP soit directement par le numéro de Sécurité sociale des intéressés soit à partir de l'état civil des personnes. À l'issue du rapprochement effectué avec le RNIPP, le numéro d'inscription au répertoire ainsi que les nom et prénom seront supprimés des fichiers d'études.

Il doit être relevé que, dans le cadre des études de mortalité différentielle présentées à la Commission, les échantillons constitués par l'INSEE, à partir d'un échantillon de 1 800 000 personnes tirées dans le recensement général de la population de 1999, concerneront un échantillon dénommé « grands âges », comprenant 200 000 personnes, hommes et femmes âgés de 85 ans et plus, un échantillon « tous âges », composé de 400 000 personnes, hommes et femmes de plus de 18 ans et un échantillon « âges actifs », composé de 1200 000 personnes âgées de 30 à 64 ans en 1999 salariées, indépendantes ou inactives.

S'agissant de la partie de l'échantillon qui concerne les personnes salariées, l'INSEE prévoit de créer cet échantillon à partir du fichier des déclarations annuelles des données sociales (DADS) qui comporte d'ores et déjà le NIR.

La constitution de l'échantillon de mortalité à partir des DADS sera réalisée en interne à l'INSEE par la division des études et enquêtes démographiques à partir d'un échantillon de mortalité des salariés composé de l'ensemble des personnes du fichier « salarié national simplifié au 25^{e} » de 1999 et d'un panel DADS au 25^{e}, composé des salariés nés un mois d'octobre d'une année paire pour étudier les relations entre mortalité et parcours professionnel et qui couvre actuellement la période 1976-1998.

Pour les échantillons précédents, la division des enquêtes et études démographiques de l'INSEE obtiendra du centre informatique d'Orléans, détenteur de la base du recensement de la population de 1999, les nom et prénom, date et lieu de naissance des individus, la situation familiale, le niveau d'instruction et la situation professionnelles, puis retransmettra ces informations au centre national informatique de Nantes qui assurera l'identification des individus au répertoire. Il sera alors procédé selon une périodicité de cinq ans à l'enrichissement des fichiers de gestion par les nouveaux décès.

Émet un avis favorable au projet de décret en Conseil d'État présenté par le ministre de l'Économie, des Finances et de l'Industrie pris en application de l'article 18 de la loi du 6 janvier 1978 et autorisant l'INSEE à utiliser le répertoire national d'identification des personnes physiques dans le cadre d'études sur la mortalité réalisées à partir d'échantillons de population.

Émet un avis favorable aux deux projets d'arrêtés présentés par le ministre de l'Économie, des Finances et de l'Industrie relatifs à des traitements automatisés d'informations individuelles mis en œuvre par l'INSEE concernant d'une part une étude de la mortalité différentielle réalisée à partir de la création d'échantillons de population issus du recensement général de 1999 et, d'autre part une étude de mortalité différentielle spécifique des salariés réalisée à partir d'un échantillon issu du fichier des déclarations annuelles des données sociales.

Délibération n° 02-111 du 19 décembre **2002 portant avis sur le projet de décret en Conseil d'État pris pour l'application du titre V de la loi n° 2002-276 du 27 février 2002**

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le Premier ministre, d'un projet de décret concernant le recensement de la population, portant création de traitements automatisés d'informations nominatives et portant application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978 ;

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

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

Vu la loi n° 51-711 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière de statistiques ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 15 et 31 ;

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

Vu la loi n° 2002-276 du 27 février 2002 relative à la démocratie de proximité, et notamment son titre V relatif aux opérations de recensement ;

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

Vu le décret n° 84-628 du 17 juillet 1984 modifié fixant les attributions, la composition et le fonctionnement du Conseil national de l'information statistique et portant application de la loi du 7 juin 1951 susvisée ;

Après avoir entendu Monsieur Guy Rosier, commissaire en son rapport et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement en ses observations ;

Formule les observations suivantes :

Aux termes de l'article 156 de la loi n° 2002-276 du 27 février 2002, le recensement de la population, effectué sous la responsabilité et le contrôle de l'Etat, a pour objet le dénombrement de la population de la France, la description des caractéristiques démographiques et sociales de la population ainsi que le dénombrement et la description des caractéristiques des logements.

Le dispositif de recensement, tel qu'il résulte de l'article 156 VI de la loi précitée, consiste à opérer par la voie d'un recensement exhaustif dans les communes comportant une population inférieure à 10 000 habitants selon un principe de rotation annuelle se déroulant sur cinq ans. Dans les communes de 10 000 habitants ou plus, une enquête par sondage est effectuée chaque année auprès de 8 % de la population totale de la commune. Au bout de cinq ans, l'ensemble du territoire de la commune a été pris en compte et 40 % de la population recensée. Le répertoire des immeubles localisés (RIL) permet, dans les communes de plus de 10 000 habitants, de répartir le territoire communal en cinq groupes d'immeubles. Chaque année, une partie des adresses d'un groupe est sélectionnée et les logements situés à ces adresses recensés.

Quelle que soit la taille des communes, pour apprécier les évolutions intervenues et appliquer celles-ci aux données collectées sur le territoire, l'article 156-VII autorise l'INSEE à utiliser des données démographiques non nominatives extraites de fichiers administratifs.

La collecte des informations est organisée et contrôlée par l'Institut national de la statistique et des études économiques (INSEE). Les enquêtes de recensement sont préparées et réalisées par les communes ou les établissements publics de coopération intercommunale (EPCI).

L'article 157-11 de la même loi de février 2002 prévoit que le recensement de la population en Nouvelle-Calédonie, en Polynésie française, à Mayotte et dans les îles Wallis et Futuna, est réalisé tous les cinq ans.

Sur les dispositions du titre II du projet de décret

Le projet de décret soumis à la Commission définit en son article 21 le champ de compétence des communes ou des EPCI et celui de l'INSEE. Les communes ou les EPCI procèdent au recensement des logements, des personnes sans abri et des personnes résidant dans des habitations mobiles terrestres présentes sur le territoire de la commune à la date de début de la collecte des données.

L'INSEE, pour sa part, est chargé de procéder au recensement des communautés et à celui des mariniers.

Le maire ou le président de l'EPCI désigne par arrêté les personnes concourant à la préparation et à la réalisation des enquêtes de recensement. Il recrute à cette fin des agents recenseurs et assure leur formation.

L'article 24. II. 1 du projet de texte prévoit que, à l'occasion de la collecte des données, des informations sont échangées entre l'INSEE et les communes ou les EPCI. Ces échanges, intervenant pendant toutes les phases de la collecte, ne portent que sur des données non nominatives. Ils n'appellent pas d'observation de la Commission.

L'article 25 du projet de décret ouvre désormais aux personnes recensées la possibilité de renvoyer leurs bulletins directement à la direction régionale de l'INSEE dont elles relèvent, et non plus directement aux communes, comme c'était le cas pour les recensements précédents. À cet égard, la Commission estime qu'il appartient à l'INSEE de porter à la connaissance de la population cette possibilité de retour direct des questionnaires à l'INSEE, que les personnes soient recensées au titre des enquêtes de recensement ou au titre des communautés.

L'article 26 énumère les données de localisation des immeubles qui sont, en application de l'article 156 de la loi précitée de 2002, nécessaires à la réalisation des enquêtes de recensement. Au titre des données de localisation des immeubles sont reprises toutes les informations figurant dans le RIL, telles qu'elles sont définies par les arrêtés du 19 juillet 2000 et du 8 novembre 2002. Au titre des données de localisation des logements figure le nom de l'occupant principal.

Cette dernière information est utile pour identifier avec certitude les logements recensés et assurer l'exhaustivité de la collecte. Elle doit par ailleurs permettre aux communes de calculer les éléments de rémunération des agents recenseurs.

// — Sur les dispositions du titre III, intitulé « Du traitement Recensement de la population »

Concernant l'intitulé du titre 111, l'emploi du *terme de* « traitement » laisse à penser que cette partie du projet de décret régit l'ensemble des traitements automatisés mis en oeuvre à l'occasion du recensement de la population. Or, les différents arti-

des du titre ne visent pas seulement des traitements mais également les opérations de collecte des données, y compris manuelles.

Il importe donc que l'intitulé soit modifié sur ce point. Il est proposé de remplacer le titre initial par le titre suivant : « Les modalités du recensement de la population ».

Il résulte de l'article 33 que le dispositif des opérations du recensement comporte cinq phases : la collecte des informations, le contrôle de l'exhaustivité des enquêtes, le contrôle de la cohérence des réponses aux enquêtes, la saisie et l'exploitation des données collectées, la diffusion des informations issues des données collectées.

Afin de lever toute ambiguïté, il est proposé que le début du premier alinéa de l'article 33 soit ainsi rédigé : « le *recensement de la population concerne les informations nominatives sur lesquelles portent les collectes d'informations mentionnées à l'article 21. Il comporte cinq phases ».*

L'article 33 prévoit que le dispositif explicité dans le titre III ne porte que sur les deux premières phases des enquêtes de recensement. Les trois dernières phases, mises en oeuvre par l'INSEE, seront autorisées par un arrêté du ministre chargé de l'Economie, après avis de la CNIL.

Toutefois s'agissant des deux premières phases, il apparaît nécessaire de préciser que celles-ci sont mises en œuvre selon des modalités définies par un arrêté pris après avis de la CNIL.

La Commission prend acte de ce que le dispositif de collecte des données diffère peu de celui du recensement de 1999. L'agent recenseur dépose les bulletins dans les logements à enquêter puis vient ensuite Tes récupérer. Les bulletins (le bulletin individuel et la feuille de logement) collectés par l'agent recenseur sont ensuite stockés par la commune ou l'EPCI puis transmis à l'INSEE dans un délai de dix jours francs après la fin de la collecte, conformément à l'article 34 du projet de décret.

L'article 34 du projet de décret fixe le délai de transmission par les communes à l'INSEE des différents documents et formulaires utilisés pour le recensement (bulletins individuels, feuilles de logement, fiche d'enquête non aboutie, carnets de tournée des agents recenseurs). Il renvoie à un arrêté du ministre de l'Économie le soin de fixer la durée de conservation de l'ensemble des données par l'INSEE. La Commission estime que l'article 34 doit être complété pour prévoir que cet arrêté sera soumis à l'avis de la CNIL.

L'article 35 du projet de décret énumère les destinataires des données lesquels sont : les personnels des communes ou des EPCI désignés par le maire ou l'organe délibérant de l'EPCI, dans les conditions prévues par l'article 22 du même projet, les personnels de l'INSEE et éventuellement les personnels des sociétés auxquelles l'INSEE pourrait faire appel.

L'article 36 organise le droit d'accès et de rectification des personnes aux données les concernant, qui s'exerce auprès des directions régionales de l'INSEE.

À l'article 38. I du projet sont énumérées les données recueillies.

Elles sont relatives :

— à la localisation des immeubles ;

— aux personnes physiques résidant dans le logement recensé : la date et le lieu de naissance, le sexe, la nationalité, la situation familiale, le niveau et la nature de la formation, les études, les activités professionnelles, le lieu de résidence, le lieu d'étude ou de travail, la résidence antérieure, les moyens de transport, les conditions de logement et l'équipement en véhicules automobiles ;

— aux caractéristiques et aux éléments de confort des logements recensés ;
— aux immeubles bâtis, année de construction et caractéristiques d'équipement.

La Commission observe que l'article 38. I. 2 doit être complété pour faire mention, au titre des données collectées, du nom et des prénoms des personnes, étant précisé, à la fin de cet alinéa, que le nom et les prénoms ne sont jamais enregistrés dans le fichier de saisie informatisé.

L'article 38. II, permet l'établissement en cas d'enquête non aboutie d'une fiche spéciale (FENA). Ce document est rempli en cas d'absence de logement à une adresse à recenser ou d'impossibilité de joindre les occupants d'un logement. Il précise la localisation et la catégorie du logement, le nom de l'occupant principal, la raison de l'impossibilité de la collecte, le nombre de personnes supposées y résider.

La Commission propose que le nom de l'occupant principal figure au titre des données énumérées à l'article 38. II dès lors que cette donnée est effectivement portée sur la fiche.

L'article 38. III autorise l'INSEE, les communes ou les EPCI à mettre en oeuvre des traitements automatisés destinés à l'avancement de la collecte. En ce qui concerne les communes ou les EPCI, ces traitements doivent également leur permettre de calculer les éléments de rémunération des agents recenseurs.

Les données enregistrées sont relatives à la localisation précise et l'identification du logement, l'état d'avancement de la collecte pour ce logement, le nom et l'identification de l'agent recenseur, la catégorie du logement, le nombre de bulletins distribués, le nombre de bulletins recueillis, la date de distribution, la date de recueil des bulletins et les dates des différents passages.

Les seuls destinataires des données sont l'INSEE, les communes ou les EPCI. S'agissant des informations sur l'agent recenseur, seules les communes ou les EPCI en ont connaissance.

La mise en œuvre de ces traitements n'appelle pas d'observation de la Commission.

L'article 39, premier alinéa, du projet de décret autorise l'INSEE, les communes ou les EPCI à créer des traitements automatisés dont la finalité est le contrôle d'exhaustivité de la collecte.

L'article 39, deuxième alinéa, leur permet d'utiliser des informations extraites du fichier de la taxe d'habitation. Les données utilisées, à cette fin de contrôle, sont relatives à la localisation précise et à la catégorie du logement, au nombre de logements par adresse et au nombre de personnes par logement.

La Commission souhaite que la procédure prévue soit encadrée par une rédaction plus précise de cet alinéa.

L'article 39, troisième alinéa, prévoit que les données nominatives détenues par les communes ou les EPCI sont détruites au plus tard trente jours francs après la date de la fin de la collecte.

La Commission demande que le troisième alinéa de l'article 39 du projet soit complété afin de rappeler que le respect du principe de finalité impose que les informations traitées à cette occasion ne seront pas utilisées à d'autres fins.

/// — Sur les dispositions de l'article 19 du titre I

L'article 19 du projet de décret vise à autoriser, en application de l'article 31 de la loi du 6 janvier 1978, à l'occasion des recensements de population, la collecte et le traitement des données nominatives susceptibles de faire apparaître l'origine ethnique des personnes en Nouvelle-Calédonie, la collecte et le traitement des

données nominatives relatives à la polygamie et au statut civil des personnes à Mayotte.

La Commission considère que :

— le recueil de l'appartenance ethnique des personnes, compte tenu des caractéris tiques socio-démographiques propres au territoire de Nouvelle-Calédonie, répond à un motif d'intérêt public au sens de l'alinéa 3 de l'article 31 de la loi du 6 janvier 1978 ;

— le recueil de la polygamie et du statut civil (personnel ou de droit commun) des personnes, qui est susceptible de faire apparaître les opinions religieuses et l'origine ethnique, compte tenu des spécificités sociales propres à la collectivité départemen tale de Mayotte, répond à un motif d'intérêt public, au sens de l'alinéa 3 de l'article 31 de la loi du 6 janvier 1978.

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

Sur l'intitulé du titre III :

— remplacer le titre initial par le titre suivant : « Les modalités du recensement de la population ».

À l'article 33 :

— rédiger ainsi le début du premier alinéa : « *Le recensement de la population concerne les informations nominatives sur lesquelles portent les collectes d'informa tion mentionnées à l'article 21. Il comporte cinq phases »* (le reste sans change ment) ;

— insérer dans la première phrase du second alinéa, après les mots *« les deux pre mières phases sont mises en œuvre »* les mots *« , selon des modalités définies par un arrêté pris après avis de la Commission nationale de l'informatique et des libertés, ».*

À l'article 34 :

— au second alinéa, insérer après les mots *« un arrêté du ministre chargé de l'Éco nomie fixe* » les mots « , après *avis de la Commission nationale de l'informatique et des libertés ».*

À l'article 38. I. 2 :

— insérer après les mots *« sur les personnes physiques et concernant »* les mots : *« le nom et les prénoms, »* ;

— compléter cet alinéa par la phrase suivante : *« le nom et les prénoms ne sont jamais enregistrés dans le fichier de saisie informatisé ; ».*

À l'article 38. II :

— compléter la deuxième phrase de ce paragraphe par les mots *« ainsi que le nom de l'occupant principal* ».

À l'article 39 :

— rédiger ainsi le second alinéa : « Ce *contrôle peut aussi être opéré à l'aide des informations énumérées à l'alinéa précédent transmises par l'administration fiscale et figurant dans le fichier de la taxe d'habitation. »* ;

— rédiger ainsi le début du troisième alinéa : *« À l'exception des données mention nées au 1 de l'article 26, les données nominatives concernées par cette phase et détenues par les communes ou les établissements publics de coopération intercom munale ne peuvent être utilisées à d'autres fins. Elles sont détruites... »* (le reste sans changement).

Émet un avis conforme aux dispositions de l'article 19 du projet de décret portant application des dispositions de l'article 31, alinéa 3, de la loi du 6 janvier 1978.

Travail

Délibération n° 02-001 du 8 janvier 2002 concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration (norme simplifiée n 42)

La Commission nationale de l'informatique et des libertés ;

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

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

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; vu le Code du travail et notamment ses articles : L. 120-2, L. 121-8, L. 143-14, L. 212-1 et suivants, L. 236-3 ; L. 412-17, L 424-3, L. 432-2-1, L. 434-1, L. 611-9, L. 620-2 ; Vu *la* loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Vu la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'État ; vu la loi n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ; Vu la loi n° 98-461 du 13 juin 1998 d'orientation et d'incitation relative à la réduction du temps de travail ;

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 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret 82-452 du 28 mai 1982 relatif aux comités techniques paritaires ; Vu le décret 2000-815 du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'Etat ;

Considérant qu'en vertu des articles 6, 17 et 21 (1°) de la loi du 6 janvier 1978 la CNIL est habilitée 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 tout dispositif qui par un élément quelconque n'est pas strictement conforme aux présentes dispositions doit faire l'objet d'une demande d'avis ou d'une déclaration ordinaire au sens des articles 15 ou 16 de la loi du 6 janvier 1978 ;

Considérant que les traitements informatisés relatifs à la gestion des contrôles d'accès aux locaux des salariés ou des agents publics et des visiteurs, à la gestion des horaires ainsi qu'à la gestion de la restauration sont de ceux qui peuvent, sous certaines conditions, relever de l'article 17 de la loi du 6 janvier 1978 ;

Considérant que les systèmes mis en œuvre peuvent utiliser la technique des cartes magnétiques ou à puce, avec ou sans contact, ou d'autres dispositifs techniques tels que, par exemple, la frappe de code secret. Les systèmes utilisant une identification biométrique sont exclus de la présente norme ;

Décide :

Article 1er :

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée de conformité à la présente norme simplifiée, les traitements automatisés d'informations nominatives visés ci-dessus doivent ne porter que sur des données objectives aisément contrôlables grâce à l'exercice du droit individuel d'accès ; ne pas donner lieu à des interconnexions avec d'autres traitements automatisés d'informations nominatives, sauf celles résultant éventuellement de l'article 5, ou à des transmissions autres que celles nécessaires à l'accomplissement des finalités énoncées à l'article 2 ; ne pas comporter d'informations autres que celles énumérées à l'article 3 ; satisfaire aux conditions énoncées aux articles 2 à 9 et ne pas mettre en œuvre de dispositifs recourant à une identification biométrique.

Les traitements mis en œuvre ne doivent concerner que les entrées et sorties du lieu de travail et ne pas permettre le contrôle des déplacements à l'intérieur du lieu de travail, à l'exception des cas dans lesquels certaines zones identifiées font l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent.

Les traitements mis en œuvre dans ce cadre n'ont pas pour objet de permettre le contrôle du respect des quotas de facilités en temps accordés aux représentants du personnel.

Article 2 : Finalités du traitement

Le traitement ne doit pas avoir d'autres finalités que :

— le contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'entreprise ou de l'administration faisant l'objet d'une restriction de circulation ;
— la gestion des horaires et des temps de présence ;
— le contrôle de l'accès au restaurant d'entreprise ou administratif et la gestion de la restauration ainsi que la mise en place d'un système de paiement associé ;
— le contrôle d'accès des visiteurs.

Article 3 : Informations collectées et traitées

Chaque application peut être mise en œuvre de façon indépendante ou intégrée. Les informations suivantes peuvent être collectées :

a) Identité : nom, prénom, numéro de matricule interne, corps d'apparte nance, grade. Photographie.

b) Vie professionnelle : service, plages horaires habituellement autorisées, zones d'accès habituellement autorisées, congés, autorisations d'absences, jours de réduction du temps de travail, décharge d'activité de service et autres absences (motifs, droits et décomptes).

c) Badges : numéro du badge ou de la carte, date de validité.

d) En cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement.

e) Visiteurs : nom, prénom, date et heure de visite, société d'appartenance et nom du salarié ou de l'agent public accueillant le visiteur.

f) Heures d'entrée et de sortie, n° de la porte utilisée.

g) En cas de gestion de la restauration, les informations relatives à la date du repas ainsi qu'au type de consommation, sous la forme exclusive : « hors d'oeuvres », « plat », « dessert », « boisson ».

h) Prix des consommations et moyen de paiement, part patronale ou de l'administration, solde.

Article 4 : Durée de conservation

Les éléments d'identification des salariés ou des agents publics ne doivent pas être conservés au-delà de cinq ans après le départ du salarié ou de l'agent de l'entreprise ou de l'administration. Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de trois mois.

Toutefois, les informations relatives aux salariés ou aux agents publics peuvent être conservées pendant cinq ans lorsque le traitement a pour finalité le contrôle du temps de travail.

La conservation des données relatives aux motifs d'absence est limitée à une durée de cinq ans sauf dispositions législatives contraires. En cas de paiement direct ou de pré-paiement des repas, les données monétiques ne peuvent être conservées plus de trois mois.

En cas de paiement par retenue sur le salaire, la durée de conservation est de cinq ans.

Article 5 : Destinataires des informations

Dans la limite de leurs attributions respectives, les informations nominatives peuvent être communiquées aux destinataires suivants :

Les personnes habilitées du service du personnel : identité, vie professionnelle, badge, temps de présence et déplacements des personnes.

Les personnes habilitées des services gérant la paie ou les traitements : identité, situation économique et financière, temps de présence, vie professionnelle.

Les personnes habilitées des services gérant la sécurité des locaux : identité, badge, temps de présence et déplacement des personnes.

Les personnes habilitées du service ou de l'organisme gérant le restaurant d'entreprise ou administratif : identité, gestion de la restauration, prix des consommations et moyen de paiement.

Lorsqu'un accord sur le temps de travail le prévoit et dans la limite des dispositions légales et conventionnelles applicables, certains salariés protégés peuvent être destinataires des informations relatives aux heures d'arrivée et de départ des personnes.

Article 6 : Liberté de circulation des salariés protégés

Les contrôles d'accès aux locaux de l'entreprise ou de l'administration et aux zones de celle-ci limitativement désignées, faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent, ne doivent pas entraver la liberté d'aller et venir des salariés protégés dans l'exercice de leurs fonctions.

Article 7 : Information et droit d'accès

Lorsque le responsable qui envisage de mettre en oeuvre un tel traitement relève des dispositions du livre IV du Code du travail relatives aux institutions représentatives des salariés au sein de l'entreprise il doit procéder à la consultation de ces institutions préalablement à la décision de mise en oeuvre du traitement.

Lorsque le responsable qui envisage de mettre en oeuvre un tel traitement relève des dispositions des lois n° 84-16 du 11 janvier 1984 portant dispositions sta-

tutaires relatives à la fonction publique de l'État, n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale et n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière, il doit procéder à l'information des comités mixtes paritaires dans les conditions prévues par l'article 15 du décret 82-452 du 28 mai 1982 relatif aux comités techniques paritaires et des articles 4 et 6 du décret 2000-815 du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'État.

L'information des salariés ou agents publics sur les finalités et les fonctions du traitement, les destinataires des informations et les modalités d'exercice de leur droit d'accès et de rectification doit être également assurée par tout moyen approprié, notamment par voie d'affichage ou par la diffusion d'une note explicative préalablement à la mise en œuvre du traitement.

Article 8 : Sécurités

Des mesures de sécurité physique et logique doivent être prises afin de préserver la sécurité du traitement et des informations, d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Article 9 :

La présente délibération sera publiée au *Journal officiel de la République française.*

Délibération n° 02-004 du 5 février 2002 portant adoption du rapport relatif à la cybersurveillance sur les lieux de travail

La Commission nationale de l'informatique et des libertés ;

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

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

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

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

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

Formule les observations suivantes :

La Commission a rendu public un rapport d'étude et de consultation publique sur la cybersurveillance des salariés dans l'entreprise le 28 mars 2001. Ce rapport a été soumis à une large consultation et de nombreuses contributions ont été apportées démontrant ainsi l'importance de ce thème dans les préoccupations des employeurs privés et publics ainsi que de leurs salariés ou agents publics.

Au bénéfice de ces observations :

— adopte le rapport relatif à la cybersurveillance sur les lieux de travail ;
— adresse ce rapport aux pouvoirs publics ainsi qu'aux organismes et associations représentatifs des acteurs concernés ;
— communique ce rapport aux autorités de contrôle des États membres de l'Union européenne réunies au sein du groupe institué par l'article 29 de la directive du 24 octobre 1995 et au président de ce groupe ;
— publie ce rapport sur le site internet de la CNIL.

Délibération n° 02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement

La Commission nationale de l'informatique et des libertés ;

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

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

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

Vu l'article 9 du Code civil ;

Vu les articles 225-1 à 225-3 ; 226-1 et 226-16 à 226-24 du Code pénal ;

Vu le Code du travail, et notamment ses articles L. 120-2, L. 121-6 à L. 121-8, L. 122-45, 123-1, L. 311-4, L. 432-2-1 et L 412-2 ;

Vu l'article L. 11.6 du Code de la route ;

Vu l'ordonnance n° 45-1030 du 24 mai 1945 relative au placement des travailleurs et au contrôle de l'emploi ;

Vu la recommandation n° 89 du Conseil de l'Europe du 18 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 81-94 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 85-044 du 15 octobre 1985 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de conseil en recrutement ;

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

La présente recommandation concerne la collecte et la gestion manuelle ou informatisée d'informations nominatives dans le cadre d'opérations de recrutement quelles soient réalisées au moyen de support électronique ou par le biais de connexion à distance. Elle abroge et remplace la précédente recommandation n° 85-044 du 15 octobre 1985.

Il convient d'entendre par opérations de recrutement, tout recrutement opéré par un intermédiaire choisi par un employeur afin de l'assister dans le choix d'une personne extérieure pour un poste à pourvoir, ainsi que tout recrutement opéré directement par un employeur partie prenante dans le choix d'une personne extérieure pour un poste à pourvoir.

Sur la nature des informations collectées relatives à la vie privée

La Commission rappelle les dispositions suivantes :

— article 1er de la loi du 6 janvier 1978 : « l'informatique doit être au service *de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »* ;

— article 9 du Code civil : *« chacun a droit au respect de sa vie privée »* ;
— article L. 120-2 du Code du travail : *« nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »* ;
— article L. 121-6 du Code du travail : *« les informations demandées sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Les informations doivent présenter un lien direct est nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles. Le candidat à un emploi […] est tenu d'y répondre de bonne foi ».*

Aussi, la Commission estime-t-elle que, de manière générale, la collecte des informations suivantes n'est pas conforme à ces dispositions légales, sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou, le cas échéant des règles en vigueur dans le pays étranger concerné par le poste : date d'entrée en France ; date de naturalisation ; modalités d'acquisition de la nationalité française ; nationalité d'origine ; numéros d'immatriculation ou d'affiliation aux régimes de Sécurité sociale ; détail de la situation militaire : sous la forme « objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade » ; adresse précédente ; entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint ainsi que nom, prénom, nationalité, profession, employeur, des parents, des beaux-parents, des frères et soeurs et des enfants) état de santé ; taille ; poids ; vue ; conditions de logement (propriétaire ou locataire) ; vie associative ; domiciliation bancaire ; emprunts souscrits.

Sur la collecte des informations

1) En application des dispositions de l'article 25 de la loi du 6 janvier 1978, la collecte de données, par tout moyen frauduleux, déloyal ou illicite est interdite.

En conséquence, serait contraire aux dispositions de cet article, l'utilisation d'annonces qui ne correspondrait pas à un poste à pourvoir, mais aurait pour seul objet de constituer un fichier de candidatures.

Constituerait de même une manœuvre déloyale, le fait, par une personne chargée du recrutement, de porter à la connaissance d'un employeur la candidature de l'un de ses salariés sans l'accord exprès de celui-ci.

La collecte de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients fournisseurs...) n'est pas contraire aux dispositions de l'article 25 de la loi du 6 janvier 1978 dès lors qu'elle n'est pas faite à l'insu du candidat. En revanche, la collecte du nom et de l'adresse de références personnelles aux fins de diligenter une enquête dite « de moralité » serait excessive et contraire à la loi.

2) En application de l'article 31 de la loi du 6 janvier 1978 et de l'article 6 de la convention 108 du Conseil de l'Europe, il est interdit de collecter et de conserver, sauf accord exprès du candidat, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales, les informations relatives à la santé ou à la vie sexuelle des personnes. L'accord exprès exigé par la loi qui doit être recueilli par écrit ne saurait, à lui seul, justifier la collecte de telles données si ces dernières sont dépourvues de lien direct et nécessaire avec l'emploi proposé. Aussi de telles informations ne peuvent-elles être collectées, sous réserve des interdictions légales, que lorsqu'elles sont justifiées par la spécificité du poste à pourvoir.

Sur l'information des personnes concernées

1°) En application des articles 26, premier alinéa et 45, deuxième alinéa de la loi du 6 janvier 1978, 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.

2°) En application des dispositions de l'article 27 de la loi du 6 janvier 1978 les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées :

— du caractère obligatoire ou facultatif des réponses ;
— des conséquences à leur égard d'un défaut de réponse ;
— des personnes physiques ou morales destinataires des informations ;
— de l'existence d'un droit d'accès et de rectification.

Lorsque de telles informations sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces prescriptions.

Il résulte en outre de l'article 10 de la directive n° 95-46 du 24 octobre 1995 que le candidat doit également être informé de l'identité du responsable du traite ment ainsi que les finalités du traitement auquel les données sont destinées.

La Commission recommande en conséquence que :

— les personnes chargées du recrutement prennent toutes les dispositions nécessai res pour informer le candidat, dans un délai raisonnable, de l'issue donnée à sa can didature, de la durée de conservation des informations le concernant ainsi que de la possibilité de demander la restitution ou la destruction de ces informations ;
— les personnes dont les coordonnées sont enregistrées dans un fichier de candidats potentiels utilisé dans le cadre d'une activité par approche directe soient informées des dispositions de l'article 27 de la loi du 6 janvier 1978, au plus tard lors du pre mier contact ;
— lorsque l'identité de l'employeur n'a pas été précisée lors de l'offre de poste, l'accord du candidat soit recueilli préalablement à la transmission des informations nominatives à cet employeur ;
— dans le cas de collecte d'informations nominatives par le biais de connexions à distance, le candidat à l'emploi soit informé de la forme, nominative ou non, sous laquelle les informations le concernant seront éventuellement diffusées en ligne ou transmises aux employeurs. Le candidat doit également être préalablement informé de toute éventuelle cession d'informations avec d'autres organismes chargés de recrutement et être en mesure de s'y opposer. Les informations collectées ne peuvent être utilisées que pour la proposition d'emploi à l'exclusion de toute autre finalité, notamment de prospection commerciale.

3°) L'article L 121-7 du Code du travail prescrit que *« le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard. […] Les résultats obtenus doivent rester confidentiels. Les méthodes et techniques d'aide au recrutement ou d'évaluation des salariés et des candidats à* un emploi doivent *être pertinentes au regard de la finalité poursuivie. »*

La Commission recommande que l'information concernant les méthodes d'aide au recrutement employées soit dispensée préalablement par écrit sous une forme individuelle ou collective.

Sur le droit d'accès et de rectification

1) En application des articles 34 et suivants, 45 de la loi du 6 janvier 1978, et L. 121-7 du Code du travail tout candidat peut obtenir communication des informations le concernant.

2) En application de l'article 36, troisième alinéa de la loi du 6 janvier 1978, en cas de contestation portant sur l'exactitude des informations, la charge de la preuve incombe au service auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord.

La Commission recommande en conséquence que tout candidat soit clairement informé des modalités d'exercice du droit d'accès et puisse obtenir sur sa demande toutes les informations le concernant y compris les résultats des analyses et des tests ou évaluations professionnelles éventuellement pratiqués.

Le droit d'accès s'applique aux informations collectées directement auprès du candidat, aux informations éventuellement collectées auprès de tiers ainsi qu'aux informations issues des méthodes et techniques d'aide au recrutement.

La Commission recommande que la communication des informations contenues dans la fiche du candidat soit effectuée par écrit, la communication des résultats des tests ou évaluations devant être faite par tout moyen approprié au regard de la nature de l'outil utilisé.

Sur la durée de conservation

En application de l'article 28 de la loi du 6 janvier 1978, sauf dispositions législatives contraires, les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la déclaration, à moins que leur conservation ne soit autorisée par la Commission.

La Commission recommande que le candidat ayant fait l'objet d'une procédure de recrutement, que cette dernière ait abouti ou non, soit informé de la durée pendant laquelle les informations le concernant seront conservées et du droit dont il dispose d'en demander, à tout moment, la suppression. En tout état de cause, la durée de conservation des informations ne devrait pas excéder deux ans après le dernier contact avec la personne concernée.

Ces recommandations sont applicables quelle que soit la forme sous laquelle les informations relatives aux candidats sont conservées, qu'il s'agisse de traitements automatisés d'informations nominatives ou de fichiers manuels ou mécanographiques.

Sur la prohibition des profils automatiques

1) En application du deuxième alinéa de l'article 2 de la loi du 6 janvier 1978, aucune décision de sélection de candidature impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement informatisé donnant une définition du profil ou de la personnalité du candidat. Dès lors, une can didature ne saurait être exclue sur le seul fondement de méthodes et techniques auto matisées d'aide au recrutement et doit faire l'objet d'une appréciation humaine.

La Commission recommande à ce titre que les outils d'évaluation automatisés à distance excluant toute appréciation humaine sur la candidature soient proscrits.

2) En application de l'article 3 de la loi du 6 janvier 1978 tout candidat a le droit d'être informé des raisonnements utilisés dans les traitements automatisés d'aide à la sélection de candidatures.

Sur les formalités préalables à l'automatisation

En application des articles 15 et 16 de la loi du 6 janvier 1978, les traitements automatisés d'informations nominatives effectués par les personnes chargées du recrutement doivent, préalablement à leur mise en œuvre, faire l'objet respectivement d'une demande d'avis ou d'une déclaration ordinaire auprès de la Commission

nationale de l'informatique et des libertés, l'omission de ces formalités préalables étant passible des sanctions prévues aux articles 226-16 à 226-24 du Code pénal.

Sur les mesures de *sécurité et de confidentialité*

En application des articles 29 et 45, de la loi du 6 janvier 1978 et L. 121-7 du Code du travail les personnes chargées du recrutement sont tenues de s'engager vis-à-vis des candidats à prendre toutes précautions utiles afin de préserver la sécurité et la confidentialité des informations, quels que soient les tests, méthodes ou techniques utilisées. Cette obligation de confidentialité s'oppose à ce que des tiers à la procédure de recrutement puissent avoir directement ou indirectement connaissance d'informations recueillies à l'occasion d'une procédure de recrutement, sauf accord préalable des intéressés. Elle n'est pas opposable aux candidats.

Délibération n° 02-018 du 21 mars 2002 portant adoption d'un modèle de questionnaire de candidature

La Commission nationale de l'informatique et des libertés ;

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

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

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

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

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

Formule les observations suivantes :

La Commission a abrogé et remplacé la recommandation n° *85-044* du 15 octobre 1985 par une délibération n° 02-017 du 21 mars 2002 portant recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

La Commission a élaboré en concertation avec le syndicat du Conseil en recrutement Syntec un questionnaire de candidature destiné à servir de modèle pour les professionnels du recrutement.

Au bénéfice de ces observations :

— adopte le modèle de questionnaire de candidature ;
— publie ce modèle sur le site internet de la CNIL.

DOSSIER DE CANDIDATURE

Ce document a été élaboré par la Commission Nationale de l'Informatique et des Libertés en collaboration avec le Syndicat du Conseil en Recrutement-Syntec. Il est destiné à servir de modèle aux cabinets de conseil en recrutement et aux entreprises au moment d'élaborer leur propre questionnaire de candidature et doit être distingué des questionnaires d'embauché. Ce questionnaire est valable pour la plupart des postes, toutefois certaines professions spécifiques (mannequin, comédien ....) peuvent nécessiter des questions complémentaires.

Nous vous prions de bien vouloir compléter soigneusement ce document, qui pourra., le cas échéant, être remis à votre futur employeur. Les réponses aux cases munies d'un astérisque sont facultatives et sans conséquence pour l'examen du dossier ; dans les autres cas, la non réponse est susceptible de compromettre le bon suivi de votre candidature.

IDENTITÉ :

Nom :
.....
Nom marital :
.....
Prénom : .....
Date de naissance :.....
Lieu de naissance* ' : .....
Nationalité : .....

Photo
D'identité

Adresse personnelle :
.....
.....
Code postal : ..... Ville : .....
Pays : .....

Téléphones où l'on peut vous joindre en toute confidentialité : .....
.....

e-mail personnel : .....

Situation de famille : seul ? en couple ?

permis de conduire : A ? B ? C ? D ? E ?

véhicule personnel : oui ? non ?

service militaire : oui ? non ?
techniques pratiquées : .....
.....
.....

coopération :.....
.....
VSNE : .....
.....

FORMATION ET CONNAISSANCES :

Baccalauréat :

Etablissement : ..... série et mention : ..... date : ..... diplôme : oui ? non ?

Etudes supérieures :

Etablissement :	nature et options :	dates :	diplôme et mention :
.....	.....	.....	oui ? non ? .....
.....	.....	.....	oui ? non ? .....
.....	.....	.....	oui ? non ? .....
.....	.....	.....	oui ? non ? .....

troisième cycle ou formation complémentaire :

Etablissement :	Nature :	Dates :	Diplôme et mention :
.....	.....	.....	oui ? non ? .....
.....	.....	.....	oui ? non ? .....

Stages :

Entreprise/ organisme :	objet :	date :	durée :
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

Langues pratiquées :

(préciser le niveau : notions, moyen, courant, bilingue)

.....

.....

.....

Séjours à l'étranger :

Dates/durée :	Pays/ville :	Motif (professionnel, tourisme, étude) :
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....

Connaissances informatiques : préciser le niveau (utilisateur, moyen/averti, expert)

Matériel :	logiciels/langages :	niveau :
.....	.....	.....
.....	.....	.....
.....	.....	.....

Autres connaissances :

.....

.....

EXPÉRIENCE PROFESSIONNELLE :

En poste actuellement : oui ? non ?
durée du préavis : .....
Réductible à : .....

En stage : oui ? non ?
date de disponibilité : .....

En préavis actuellement : oui ? non ?
date de disponibilité : .....

Clause de non-concurrence : oui ? non ?
durée et limites .....
.....
La dernière société employeur est-elle
filiale d'un groupe : oui ? non ?
Nom du groupe : .....
Nationalité : .....
Effectif : .....
CA : .....

Expérience professionnelle	**Fonction actuelle ou dernière fonction** Du ..... au	**Fonction précédente** Du..... au .....
Société :		
Adresse		
Effectif et CA		
Secteur d'activité		
Votre fonction et son secteur géographique éventuel		
Votre mission		
Votre rattachement hiérarchique		
Personnes encadrées Nombre et niveau		
Vos réalisations et résultats		
Rémunération actuelle brute annuelle	Fixe : ..... Variable : ..... Voiture ? autre ?	

Fonctions antérieures	Du..... au	Du ..... au .....
Société et adresse		
Mission, fonctions		
Secteur d'activité		

Emplois antérieurs : oui ? non ?
Nombre : .....
Année du premier emploi :.....
Durées respectives : .....
.....

Sociétés auxquelles votre dossier ne doit pas être présenté :
.....
.....

MOTIVATIONS :

Quels sont les motifs de votre recherche et vos objectifs de carrière :
.....
.....
.....

Rémunération annuelle brute souhaitée (fixe et variable) :.....

Disponibilité pour voyager : oui ? nombre maximum de jours par mois :
Si non ? raisons* :..... .....

Changement de résidence : possible ? non envisageable pour l'instant ? non ?
Si non raisons* :
Profession du conjoint ? scolarité des enfants ? attachement au lieu de résidence ?

Implantations géographiques souhaitées (par ordre de préférence) :

.....

Expatriation acceptée : oui ? non ? pays : .....
Zones exclues : .....

Références professionnelles :

De préférence vos anciens supérieurs hiérarchiques qui pourront être consultés en fin de processus avec votre cord.

Nom :.....	.....	.....
Prénom :.....	.....	.....
Fonction :.....	.....	.....
Société :	.....	.....
Adresse :	.....	.....
Téléphone :	.....	.....

Loisirs* :
.....

Conformément à l'article L 121-7 du code du travail, nous vous informons que la procédure de recrutement utilisée par notre cabinet/entreprise comprend : des entretiens, éventuellement une analyse graphologique et/ou des tests psychotechniques. Les résultats de ces tests vous seront restitués sur demande auprès de notre cabinet/service recrutement de façon écrite/orale, ils ne seront conservés dans votre dossier qu'en cas de présentation à l'entreprise/embauche dans l'entreprise.

Nous vous informons que les données vous concernant sont (ne sont pas) informatisées, elles seront traitées de façon confidentielle. Conformément aux articles 34, 36 et 45 de la loi du 6 janvier 1978, nous vous informons que vous disposez d'un droit d'accès , de rectification et de suppression aux informations vous concernant, pour
ce faire il suffit de vous adresser auprès du service .....
J'autorise le cabinet ..... à communiquer les informations me concernant à toute
entreprise cliente, à l'exception des entreprises mentionnées ci-dessus. Oui ? non ?
J'autorise le cabinet/l'entreprise ..... à communiquer les informations me concernant aux autres filiales du groupe situées en dehors de l'Union Européenne. Oui ? non ?

Fait le ..... à .....

Signature :

Délibération n° 02-106 du 19 décembre 2002 portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article L 133-5 du Code de la Sécurité sociale concernant l'utilisation du NIR dans le cadre des télédéclarations effectuées sur le portail www.net-entreprises.fr

La Commission nationale de l'informatique et des libertés ;

Saisie pour avis par le ministère des Affaires sociales, du Travail et de la Solidarité d'un projet de décret pris en application de l'article L. 133-5 du Code de la Sécurité sociale ;

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

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

Vu le Code de la Sécurité sociale et le Code du travail ;

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 susvisée ;

Vu les demandes d'avis présentées par le groupement d'intérêt public « modernisation des déclarations sociales » pour la mise en œuvre des téléservices net-DUCS-I (n° 829385), net-DADS-U (n° 829386) et net-DCR (n° 829387) ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire en son rapport, et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement en ses observations ;

Formule les observations suivantes :

La loi de financement de la sécurité sociale pour 2002 a introduit dans le Code de la Sécurité sociale un article L. 133-5 afin de permettre aux employeurs et aux professions indépendantes de réaliser leurs déclarations sociales obligatoires par voie électronique et de bénéficier d'un service d'aide à l'élaboration des déclarations sociales et des bulletins de paie baptisé « DUCS-I » (déclaration unifiée de cotisations sociales individualisée).

Le groupement d'intérêt public « modernisation des déclarations sociales » (GIP-MDS) a été choisi par les organismes gestionnaires de régimes de protection sociale pour gérer ce service dans le cadre du portail de téléservices www.net-entreprises.fr déjà mis en œuvre par ce groupement.

L'article L. 133-5 du Code de la Sécurité sociale prévoit que, pour assurer ce service et sa sécurisation, les organismes sociaux ou un organisme désigné par eux — en l'occurrence, le GIP-MDS — sont autorisés à collecter et conserver le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) des personnes concernées, dans des conditions fixées par décret en Conseil d'État pris après avis de la CNIL.

La Commission est donc amenée à se prononcer sur les garanties apportées par le projet de décret qui lui est soumis par le ministère des Affaires sociales, du Travail et de la Solidarité, sur la base des éléments transmis par le ministère et par le

GIP-MDS dans le cadre de trois demandes d'avis concernant les téléservices net-DUCS-I, net-DADS-U et net-DCR.

Sur les finalités d'utilisation du NIR

Les articles 1 et 2 du projet de décret prévoient d'introduire une modification des articles R. 115-1 et R. 115-2 du Code de la Sécurité sociale afin de définir limitativement les organismes susceptibles d'utiliser le NIR dans le cadre des téléprocédures visées à l'article L. 133-5 du même Code.

Seraient ainsi autorisés à utiliser le NIR dans le cadre du dispositif net-entreprises les organismes chargés de la gestion d'un régime obligatoire de base de la sécurité sociale (déjà visés au 1° de l'article R. 115-1), les organismes visés par les articles L. 223-16 (caisses de congés payés) et L. 351-2 (UNEDIC et ASSEDIC) du Code du travail, ainsi que le GIP-MDS en tant qu'organisme désigné par les organismes de protection sociale précités pour gérer ce dispositif.

La Commission observe que les organismes visés par les articles 1 et 2 du projet de décret sont expressément habilités par l'article L. 133-5 du Code de la Sécurité sociale à recevoir les déclarations obligatoires des employeurs ou des cotisants, qui intègrent le NIR, par le téléservice net-entreprises.

La Commission prend acte de ce que le NIR ne serait ni utilisé dans le cadre de l'inscription aux différents téléservices du portail net-entreprises, ni dans le cadre de la procédure actuelle d'authentification des utilisateurs de ces téléservices, mais uniquement pour l'établissement des déclarations sociales nécessitant le recueil du NIR.

La Commission a toutefois été informée de la réalisation d'une étude visant à la mise en œuvre, dans le cadre du programme net-entreprises, d'un procédé d'authentification des déclarants reposant sur l'émission de certificats électroniques personnels normalisés, projet dans lequel l'utilisation du NIR personnel de l'employeur pourrait ne pas être exclue.

La Commission estime qu'une utilisation du NIR à de telles fins ne peut qu'appeler de sa part une réserve de principe dans la mesure où la concrétisation d'un tel projet constituerait un précédent en faveur de l'utilisation généralisée de cet identifiant particulier dans le cadre de dispositifs de certificats électroniques délivrés aux citoyens souhaitant acheter ou vendre sur internet, voter à distance, consulter leur e-dossier, etc., et aurait pour conséquence la constitution, par les sociétés de certification prestataires, de bases de données contenant les références de plusieurs millions d'employeurs ou de leurs délégataires identifiés par leur NIR.

Sur les conditions de traitement du NIR

L'article 3 du projet de décret précise que la collecte des informations traitées dans le cadre de la DUCS-I., dont le NIR, seraient recueillies par le GIP-MDS soit directement auprès des déclarants, soit auprès des organismes sociaux lorsqu'une procédure de pré-établissement des déclarations par les organismes sociaux concernés est prévue.

L'article 4 prévoit que la transmission électronique de ces informations ferait l'objet d'un chiffrement.

L'article 5 prévoit que la collecte et la conservation des données devraient être réalisées dans des conditions qui permettent d'en assurer leur sécurité. Afin de s'assurer de la mise en oeuvre de moyens adéquats pour atteindre cet objectif, la Commission serait rendue destinataire chaque année d'un rapport d'évaluation de la sécurité du dispositif, rapport dont la Direction centrale de la sécurité des systèmes d'information serait également rendue destinataire.

Enfin, l'article 6 prévoit que les informations recueillies dans le cadre des téléservices visés à l'article L. 133-5 du Code de la Sécurité sociale seront conservées, pour chaque déclaration concernée, jusqu'à extinction des délais de recours contentieux ou pendant trente jours s'agissant des déclarations entrant dans le champ de la DADS-U, date à laquelle elles feront l'objet d'un archivage définitif dans les conditions prévues par la loi du 3 janvier 1979 sur les archives.

La Commission prend acte de ces dispositions. Elle considère cependant que l'intention du législateur n'a pas été de limiter les garanties apportées autour du traitement du NIR au seul cadre du téléservice DUCS-I et qu'il convient, en conséquence, d'étendre ces garanties à l'ensemble des téléservices mis en oeuvre sur le fondement de l'article L. 133-5 du Code de la Sécurité sociale nécessitant une utilisation du NIR des personnes concernées.

Émet un avis favorable au projet de décret sous réserve que :

L'article 3 soit ainsi rédigé : *« Les informations nécessaires à la mise en œuvre des services prévus par l'article L. 133-5 du Code de la Sécurité sociale sont collectées par le groupement d'intérêt public »* Modernisation des déclarations sociales « *directement auprès des déclarant ou de leurs mandataires ou, le cas échéant, recueillies auprès des organismes constituant le groupement. »* ;

L'article 5 soit ainsi rédigé : « *Le groupement d'intérêt public* » Modernisation des déclarations sociales *« collecte et conserve les données qu'il recueille, dans le cadre de ces services, dans des conditions qui permettent d'en assurer leur sécurité ».*

Il rend compte chaque année des conditions dans lesquelles la sécurisation de la collecte et la conservation des données est assurée, au moyen d'un rapport d'évaluation remis à la Commission nationale de l'informatique et des libertés et à la Direction centrale de la sécurité des systèmes d'information. Le premier rapport sera établi un an après la mise en œuvre des services.

Délibération n° 02-107 du 19 décembre 2002 relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DUCS-I sur le portail www.net-entreprises.fr

La Commission nationale de l'informatique et des libertés ;

Saisie par le groupement d'intérêt public « modernisation des déclarations sociales » de trois demandes d'avis concernant la mise en œuvre des téléservices net-DUCS-I (n° 829385), net-DADS-U (n° 829386) et net-DCR (n° 829387) prévus à l'article L. 133-5 du Code de la Sécurité sociale ;

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

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

Vu le Code de la Sécurité sociale et le Code du travail ;

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 susvisée ;

Vu le projet de décret d'application de l'article L. 133-5 du Code de la Sécurité sociale soumis concomitamment par le ministère des Affaires sociales, du Travail et de la Solidarité (saisine n° 02013599) ;

Vu l'article 21 de la convention constitutive du groupement d'intérêt public « modernisation des déclarations sociales » du 21 février 2000, approuvée par arrêté interministériel du 17 mars 2000, autorisant son directeur à représenter le groupement ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire en son rapport, et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement en ses observations ;

Formule les observations suivantes :

La loi de financement de la sécurité sociale pour 2002 a introduit dans le Code de la Sécurité sociale un article L. 133-5 afin de permettre aux employeurs et aux professions indépendantes de réaliser leurs déclarations sociales obligatoires par voie électronique et de bénéficier d'un service d'aide à l'élaboration des déclarations sociales et des bulletins de paie baptisé « DUCS-I » (déclaration unifiée de cotisations sociales individualisée).

Le groupement d'intérêt public « modernisation des déclarations sociales » (GIP-MDS) a été choisi par les organismes gestionnaires de régimes de protection sociale pour gérer ces téléservices dans le cadre du portail www.net-entreprises.fr déjà mis en œuvre par ce groupement.

La Commission est amenée à se prononcer sur une demande d'avis présentée par le GIP-MDS concernant la mise en œuvre du téléservice net-DUCS-I.

Sur la finalité du traitement et les destinataires des informations nominatives

Créé par l'article L. 133-5 du Code de la Sécurité sociale, le téléservice net-DUCS-I est destiné à simplifier les déclarations des entreprises en regroupant, en

une déclaration unique, l'ensemble des obligations déclaratives des employeurs en matière de déclarations de cotisations sociales : établissement de la déclaration unifiée de cotisations sociales (DUCS), acquittement du montant des cotisations par téléréglement, élaboration de déclarations connexes (DADS, attestation employeur...) et enfin aide à l'élaboration des bulletins de paie.

Les différentes phases de traitement des informations nominatives nécessaires à l'établissement de la DUCS-I seront les suivantes :

— inscription de l'établissement à net-entreprises (en se connectant sur www.net-entreprises.fr) ;

— inscription au service DUCS-I (sélection des organismes de protection sociale des tinataires des déclarations et des comptes bancaires à utiliser pour le téléréglement, vérification de l'appartenance de l'établissement au périmètre DUCS-I) ;

— inscription des salariés de l'établissement au service DUCS-I par le déclarant ;

— calcul mensuel du montant des cotisations dues sur le mois pour chacun des sala riés ;

— aide à l'édition chaque mois d'une fiche de calcul des cotisations sociales et d'un bulletin de paie par salarié ;

— calcul et envoi en fin de trimestre de la déclaration des cotisations sociales (décla ration de masse non nominative) de l'établissement pour chaque organisme de pro tection sociale destinataire (URSSAF, Assedic, CCP BTP, ARRCO, AGIRC, institutions de prévoyance) ;

— envois du paiement des cotisations par téléréglement en fin de trimestre (un paie ment par organisme de protection sociale) ;

— et d'ici la fin de l'année 2003, envois en fin d'année de la déclaration annuelle à chaque organisme de protection sociale destinataire.

Sur la pertinence des données traitées

Le NIR sera utilisé dans le cadre de cette télédéclaration afin de contribuer à l'identification des salariés concernés.

La Commission observe que cette utilisation ne soulève pas de difficulté dans la mesure où, d'une part, le décret n° 91-1404 du 27 décembre 1991 pris après avis de la CNIL prévoit que les employeurs publics ou privés sont autorisés à utiliser le NIR pour les opérations de déclarations sociales et, d'autre part, l'article L. 133-5 du Code de la Sécurité sociale et le projet de décret soumis concomitamment à la Commission par le ministère du Travail ont précisément pour objet d'autoriser le traitement du NIR par le GIP-MDS dans le strict cadre de la réalisation des déclarations sociales par voie électronique.

Les catégories d'informations traitées seront celles déjà recueillies dans le cadre des déclarations obligatoires existantes, auxquelles seront ajoutées des données permettant d'apporter une aide à l'élaboration des bulletins de paie des salariés concernés, et en particulier des informations relatives à la situation familiale des salariés.

La collecte de cette dernière donnée ne sera opérée qu'auprès des déclarants ayant préalablement indiqué relever d'un régime de prévoyance pour lequel cette donnée est nécessaire.

Dans ces conditions, la Commission n'a pas d'observation à formuler sur la pertinence des données traitées.

Sur les sécurités mises en œuvre

Le téléservice net-DUCS-I devrait entraîner la constitution par le GIP-MDS d'une base de données nominatives sur les salariés des entreprises ayant souhaité adhérer au dispositif.

Dès lors, la Commission considère que la sécurisation des échanges, des sessions de télédéclaration ou de consultation, et du stockage des données est un objectif qui revêt en l'espèce une importance particulière.

La Commission observe à cet égard que l'hébergement des différents sites Internet du dispositif net-entreprises est réparti entre la CNAVTS (pour l'inscription des déclarants), la société Matra global net services (pour la gestion du site portail www.net-entreprises.fr) et la société France Telecom-Equant (pour l'hébergement des sites déclaratifs).

La Commission prend acte des mesures de sécurité physiques et logiques adoptées pour garantir la confidentialité et l'intégrité des données traitées dans le cadre du service DUCS-I.

La Commission estime néanmoins que le dispositif de journalisation des connexions existant devrait être amélioré en prévoyant une exploitation régulière des données de connexion et un recueil de données sur la nature des opérations effectuées à chaque connexion de façon à permettre une détection et une correction d'éventuelles intrusions dans le système d'information.

La Commission relève par ailleurs que le GIP-MDS met en œuvre une procédure de jeton sécurisé après authentification des déclarants par « login » et mot de passe afin de sécuriser l*es* sessions d'accès au téléservice.

La Commission n'a pas, en l'état, d'observations à formuler sur le dispositif d'authentification par « login » et mot de passe aujourd'hui déployé par le GIP-MDS, sans préjudice des avis ou recommandations qu'elle sera amenée à émettre ultérieurement sur le recours à des dispositifs alternatifs.

A cet égard, la Commission observe qu'une étude est en cours de réalisation par le GIP-MDS visant à la mise en oeuvre, dans le cadre du programme net-entreprises, d'un procédé d'authentification des déclarants reposant sur l'émission de certificats électroniques personnels normalisés, projet dans lequel l'utilisation du NIR de l'employeur ne serait pas exclue.

La Commission estime qu'une utilisation du NIR à de telles fins ne peut qu'appeler de sa part une réserve de principe dans la mesure où la concrétisation un tel projet constituerait un précédent en faveur de l'utilisation généralisée de cet identifiant particulier dans le cadre de dispositifs de certificats électroniques délivrés aux citoyens souhaitant acheter ou vendre sur Internet, voter à distance, consulter leur e-dossier, etc., et aurait pour conséquence la constitution, par les sociétés de certification prestataires, de bases de données contenant les références de plusieurs millions d'employeurs ou de leurs délégataires identifiés par leur NIR.

Enfin, la Commission considère que la sécurité du traitement devrait être renforcée sur le plan juridique par l'intégration dans les contrats de prestation de service, au-delà des clauses de confidentialité et de réversibilité déjà introduites, d'une clause de non-détournement de finalité.

Sur les durées de conservation des données

Le GIP-MDS assurera un service d'archivage des déclarations au bénéfice des déclarants et des organismes sociaux pendant une durée de trois années à compter de la date à laquelle les sommes dues au titre des cotisations concernées par net-DUCS-I deviennent exigibles.

La Commission considère que cette durée n'est pas excessive au regard des finalités poursuivies.

Sur l'information des personnes concernées

L'information des déclarants sera réalisée sur le site www.net-entreprises.fr et notamment sur les pages où la collecte des informations nominatives sera opérée.

Dans la mesure où cette information ne pourra être reçue que par les personnes chargées des déclarations des entreprises, alors même que les traitements concernent au premier chef les salariés de ces entreprises, la Commission considère qu'il convient de rappeler aux entreprises leur obligation d'informer leurs salariés de la transmission d'informations les concernant aux organismes sociaux par net-DUCS-I, conformément à l'article 27 de la loi du 6 janvier 1978.

Émet on avis favorable à la demande d'avis présentée par le GIP-MDS sous réserve que :

— le dispositif de journalisation des connexions existant prévoie une exploitation régulière des données de connexion et un recueil de données sur la nature des opéra tions effectuées à chaque connexion ;

— une clause de non-détournement de finalité soit intégrée dans le contrat liant le GIP-MDS à l'entreprise assurant l'hébergement du site net-DUCS-I.

Demande à être rendue destinataire d'un bilan de la mise en oeuvre du téléservice dans un délai d'un an.

Délibération n° 02-108 du 19 décembre 2002 relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DADS-U sur le portail www.net-entreprises.fr

La Commission nationale de l'informatique et des libertés ;

Saisie par le groupement d'intérêt public « modernisation des déclarations sociales » de trois demandes d'avis concernant la mise en oeuvre des téléservices net-DUCS-I (n° 829385), net-DADS-U (n° 829386) et net-DCR (n° 829387) prévus à l'article L. 133-5 du Code de la Sécurité sociale ;

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

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

Vu le Code de la Sécurité sociale et le Code du travail ; 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 susvisée ;

Vu le projet de décret d'application de l'article L. 133-5 du Code de la Sécurité sociale soumis concomitammenî par le ministère des Affaires sociales, du Travail et de la Solidarité (saisine n° 02013599) ;

Vu l'article 21 de la convention constitutive du groupement d'intérêt public « modernisation des déclarations sociales » du 21 février 2000, approuvée par arrêté interministériel du 17 mars 2000, autorisant son directeur à représenter le groupement ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire en son rapport, et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement en ses observations ;

Formule les observations suivantes :

La loi de financement de la sécurité sociale pour 2002 a introduit dans le Code de la Sécurité sociale un article L. 133-5 afin de permettre aux employeurs et aux professions indépendantes de réaliser leurs déclarations sociales obligatoires par voie électronique et de bénéficier d'un service d'aide à l'élaboration des déclarations sociales et des bulletins de paie.

Le groupement d'intérêt public « modernisation des déclarations sociales » (GIP-MDS) a été choisi par les organismes gestionnaires de régimes de protection sociale pour gérer ces téléservices dans le cadre du portail www.net-entreprises.fr déjà mis en œuvre par ce groupement.

La Commission est amenée à se prononcer sur une demande d'avis présentée par le GIP-MDS concernant la mise en œuvre du téléservice net-DADS-U.

Sur la finalité du traitement et les destinataires des informations nominatives

La déclaration automatisée de données sociales unifiée « DADS-U » est le fruit d'une réflexion conduite depuis plusieurs années par la CNAVTS et les fédérations de retraite complémentaire AGIRC et ARRCO afin de regrouper en une déclara-

tion unique la déclaration annuelle de données sociales (DADS) mise en œuvre par la CNAVTS pour le compte des partenaires du dispositif « transfert de données sociales (TDS) » et la déclaration annuelle de données sociales des caisses de retraite complémentaire (DADS-CRC) à destination des institutions de retraite complémentaire et les institutions de prévoyance.

L'article L. 133-5 du Code de la Sécurité sociale et l'arrêté du 29 juillet 2002 pris pour son application permettent le traitement par voie électronique de cette déclaration unifiée.

Les traitements d'informations nominatives opérés dans le cadre de net-DADS-U seront les suivants :
— inscription au téléservice ;
— transfert de fichiers de données personnelles des déclarants vers net-DADS-U ;
— contrôle de conformité des fichiers reçus à la norme DADS-U ;
— filtrage et transmission aux organismes de protection sociale partenaires (chaque partenaire ne reçoit que les informations le concernant) ;
— consultation par le déclarant du bilan des contrôles de conformité effectués par le site ;
— destruction des déclarations au bout de trente jours et stockage des bilans des contrôles de conformité sur une année.

Sur la pertinence des données traitées

Le formulaire de collecte des données DADS-U a été défini sur la base du cahier technique et du guide d'utilisation DADS-U (norme DADS-U V06 R02), dans le respect des textes réglementaires relatifs au dispositif « transfert de données sociales ».

Le NIR sera utilisé dans le cadre de cette télédéclaration afin de contribuer à l'identification des salariés concernés.

L'ensemble des organismes sociaux sont autorisés par les articles R. 115-1 et R. 115-2 du Code de la Sécurité sociale à détenir le NIR de leurs ressortissants dans leurs fichiers.

La Commission observe également que cette utilisation du NIR ne soulève pas de difficulté dans la mesure où, d'une part, le décret n° 91-1404 du 27 décembre 1991 pris après avis de la CNIL prévoit que les employeurs publics ou privés sont autorisés à utiliser cet identifiant pour les opérations de déclarations sociales et, d'autre part, l'article L. 133-5 du Code de la Sécurité sociale et le projet de décret soumis concomitamment à la Commission par le ministère du Travail ont précisément pour objet d'autoriser le traitement du NIR par le GIP-MDS dans le strict cadre de la réalisation des déclarations sociales par voie électronique.

Le NIR serait également utilisé au sein des bilans d'anomalies produits dans le cadre des contrôles de conformité à la norme DADS-U dans les cas où l'anomalie serait relative à une information au niveau du salarié (le bilan préciserait uniquement les nom et prénom et NIR du salarié concerné). La Commission considère que cette intégration du NIR dans les bilans ne soulève pas de difficultés compte tenu du fait que seuls les personnels habilités de l'entreprise déclarante ou de l'organisme de protection sociale concernés pourrait ainsi accéder aux bilans relatifs à cette entreprise afin de faciliter la correction des erreurs liées à la situation d'un salarié pour la bonne prise en compte de ses droits par les organismes sociaux.

Les catégories d'informations traitées seront celles déjà recueillies dans le cadre des déclarations obligatoires existantes, et en particulier des informations relatives à la situation familiale des salariés.

La collecte de cette dernière donnée ne serait opérée qu'auprès des déclarants ayant préalablement indiqué relever d'un régime de prévoyance pour lequel cette donnée est nécessaire.

Dans ces conditions, la Commission n'a pas d'observation à formuler sur la pertinence des données traitées.

Sur les sécurités mises en œuvre

Le téléservice net-DADS-U devrait entraîner la constitution par le GIP-MDS d'une base de données nominatives sur les salariés des entreprises ayant souhaité adhérer au dispositif.

Dès lors, la Commission considère que la sécurisation des échanges, des sessions de télédéclaration ou de consultation, et du stockage des données est un objectif qui revêt en l'espèce une importance particulière.

La Commission observe à cet égard que l'hébergement des différents sites Internet du dispositif net-entreprises est réparti entre la CNAVTS (pour l'inscription des déclarants), la société Matra global net services (pour la gestion du site portail www.net-entreprises.fr) et la société France Telecom-Equant (pour l'hébergement des sites déclaratifs).

La Commission prend acte des mesures de sécurité physiques et logiques adoptées pour garantir la confidentialité et l'intégrité des données traitées dans le cadre du service DADS-U.

La Commission estime néanmoins que le dispositif de journalisation des connexions existant devrait être amélioré en prévoyant une exploitation régulière des données de connexion et un recueil de données sur la nature des opérations effectuées à chaque connexion de façon à permettre une détection et une correction d'éventuelles intrusions dans le système d'information.

La Commission relève par ailleurs que le GIP-MDS met en œuvre une procédure de jeton sécurisé après authentification des déclarants par « login » et mot de passe afin de sécuriser les sessions d'accès au téléservice.

La Commission n'a pas, en l'état, d'observations à formuler sur le dispositif d'authentification par « login » et mot de passe aujourd'hui déployé par le GIP-MDS, sans préjudice des avis ou recommandations qu'elle sera amenée à émettre ultérieurement sur le recours à des dispositifs alternatifs.

À cet égard, la Commission observe qu'une étude est en cours de réalisation par le GIP-MDS visant à la mise en œuvre, dans le cadre du programme net-entreprises, d'un procédé d'authentification des déclarants reposant sur l'émission de certificats électroniques personnels normalisés, projet dans lequel l'utilisation du NIR ne serait pas exclue.

La Commission estime qu'une utilisation du NIR à de telles fins ne peut qu'appeler de sa part une réserve de principe dans la mesure où la concrétisation d'un tel projet constituerait un précédent en faveur de l'utilisation généralisée de cet identifiant particulier dans le cadre de dispositifs de certificats électroniques délivrés aux citoyens souhaitant acheter ou vendre sur Internet, voter à distance, consulter leur e-dossier, etc., et aurait pour conséquence la constitution, par les sociétés de certification prestataires, de bases de données contenant les références de plusieurs millions d'employeurs ou de leurs délégataires identifiés par leur NIR.

Enfin, la Commission considère que la sécurité du traitement devrait être renforcée sur le plan juridique par l'intégration dans les contrats de prestation de service, au-delà des clauses de confidentialité et de réversibilité déjà introduites, d'une clause de non-détournement de finalité.

Sur les durées de conservation des données

Le GIP-MDS assurera la destruction des données recueillies dans le cadre du téléservice net-DADS-U trente jours après la déclaration, et le stockage des bilans des contrôles de conformité après une année.

La Commission considère que ces durées ne sont pas excessives au regard des finalités poursuivies.

Sur l'information des personnes concernées

L'information des déclarants sera réalisée sur le site www.net-entreprises.fr et notamment sur les pages où la collecte des informations nominatives sera opérée.

Dans la mesure où cette information ne pourra être reçue que par les personnes chargées des déclarations des entreprises, alors même que les traitements concernent au premier chef les salariés de ces entreprises, la Commission considère qu'il convient de rappeler aux entreprises leur obligation d'informer leurs salariés de la transmission d'informations les concernant aux organismes sociaux par net-DADS-U, conformément à l'article *17* de la loi du 6 janvier 1978.

Émet un avis favorable à la demande d'avis présentée par le GIP-MDS sous réserve que :

— le dispositif de journalisation des connexions existant prévoie une exploitation régulière des données de connexion et un recueil de données sur la nature des opéra tions effectuées à chaque connexion ;

— une clause de non-détournement de finalité soit intégrée dans le contrat liant le GIP-MDS à l'entreprise assurant l'hébergement du site net-DADS-U ;

Demande à être rendue destinataire d'un bilan de la mise en œuvre du téléservice dans un délai d'un an.

Délibération n° 02-109 du 19 décembre 2002 relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DCR sur le portail www.net-entreprises.fr

La Commission nationale de l'informatique et des libertés ;

Saisie par le groupement d'intérêt public « modernisation des déclarations sociales » de trois demandes d'avis concernant la mise en œuvre des téléservices net-DUCS-I (n° 829385), net-DADS-U (n° 829386) et net-DCR (n° 829387) prévus à l'article L. 133-5 du Code de la Sécurité sociale ;

Vu la directive n° *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 ;

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 de la Sécurité sociale et le Code du travail ;

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 susvisée ;

Vu le projet de décret d'application de l'article L. 133-5 du Code de la Sécurité sociale soumis concomitamment par le ministère des Affaires sociales, du Travail et de la Solidarité (saisine n° 02013599) ;

Vu l'article 21 de la convention constitutive du groupement d'intérêt public « modernisation des déclarations sociales » du 21 février 2000, approuvée par arrêté interministériel du 17 mars 2000, autorisant son directeur à représenter le groupement ;

Après avoir entendu Monsieur Hubert Bouchet, commissaire en son rapport, et Madame Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement en ses observations ;

Formule les observations suivantes :

La loi de financement de la Sécurité sociale pour 2002 a introduit dans le Code de la Sécurité sociale un article L. 133-5 afin de permettre aux employeurs et aux professions indépendantes de réaliser leurs déclarations sociales obligatoires par voie électronique et de bénéficier d'un service d'aide à l'élaboration des déclarations sociales et des bulletins de paie.

Le groupement d'intérêt public « modernisation des déclarations sociales » (GIP-MDS) a été choisi par les organismes gestionnaires de régimes de protection sociale pour gérer ces téléservices dans le cadre du portail www.net-entreprises.fr déjà mis en œuvre par ce groupement.

La Commission est amenée à se prononcer sur une demande d'avis présentée par le GIP-MDS concernant la mise en œuvre du téléservice net-DCR.

Sur la finalité du traitement et les destinataires des informations nominatives Le téléservice net-DCR permettra la numérisation de la déclaration commune des revenus des professions indépendantes existant sur support papier (sans entraî-

ner de modification sur le fond) et la simplification de la procédure déclarative (grâce à un pré-remplissage des déclarations).

L'article L. 133-5 du Code de la Sécurité sociale et l'arrêté du 29 juillet 2002 pris pour son application permettent le traitement par voie électronique de cette déclaration.

Les traitements d'informations nominatives opérés dans le cadre de net-DCR seront les suivants :

— inscription au téléservice ;

— amorçage des déclarations (la CANAM envoie au site les données connues de son système d'information nécessaires au pré-remplissage des déclarations et à leur contrôle) ;

— déclaration par EFI (saisie des données sur un formulaire préalablement person nalisé avec les données transmises par la CANAM) ;

— contrôle de forme et production d'un accusé de réception (qui dégage le décla rant de son obligation déclarative) ;

— transmission des données à la CANAM qui les retransmet aux organismes parte naires DCR ;

— historisation des déclarations sur le site net-DCR sur quatre années (afin de per mettre aux déclarants d'apporter aisément la preuve du contenu de leur déclaration durant les délais de prescription légaux) ;

— traçabilité des actions opérées sur le site.

Les destinataires finaux des informations n'excéderont pas ceux déjà visés dans les dossiers relatifs à la DCR antérieurement soumis à la Commission, à savoir les gestionnaires nationaux et locaux de la CANAM, de l'ACOSS, de l'ORGANIC et de la CANCAVA.

Sur la pertinence des données traitées

Le NIR sera utilisé afin de contribuer à l'identification des cotisants par les organismes sociaux partenaires dans la mesure où certains travailleurs indépendants ont plusieurs SIRET correspondant à leurs différentes activités.

La Commission observe que les articles R. 115-1 et R. 115-2 du Code de la Sécurité sociale autorisent l'ensemble des organismes sociaux partenaires de net-DCR à utiliser le NIR.

S'agissant des autres catégories d'informations traitées dans le cadre de net-DCR, celles-ci apparaissent conformes aux données figurant dans le modèle du formulaire « déclaration commune des revenus des professions indépendantes pour l'année 2002 » fixé par un arrêté du 25 avril 2002.

Dans ces conditions, la Commission n'a pas d'observation à formuler sur la pertinence des données traitées.

Sur les sécurités mises en œuvre

Le téléservice net-DCR devrait entraîner la constitution par le GIP-MDS d'une base de données nominatives sur les professions indépendantes ayant souhaité adhérer au dispositif.

Dès lors, la Commission considère que la sécurisation des échanges, des sessions de télédéclaration ou de consultation, et du stockage des données est un objectif qui revêt en l'espèce une importance particulière.

La Commission observe à cet égard que l'hébergement des différents sites Internet du dispositif net-entreprises est réparti entre la CNAVTS (pour l'inscription des déclarants), la société Matra global net services (pour la gestion du site portail

www.net-entreprises.fr) et la société France Telecom-Equant (pour l'hébergement des sites déclaratifs).

La Commission prend acte des mesures de sécurité physiques et logiques adoptées pour garantir la confidentialité et l'intégrité des données traitées dans le cadre du service net-DCR.

La Commission estime néanmoins que le dispositif de journalisation des connexions existant devrait être amélioré en prévoyant une exploitation régulière des données de connexion et un recueil de données sur la nature des opérations effectuées à chaque connexion de façon à permettre une détection et une correction d'éventuelles intrusions dans le système d'information.

La Commission relève par ailleurs que le GIP-MDS met en œuvre une procédure de jeton sécurisé après authentification des déclarants par « login » et mot de passe afin de sécuriser les sessions d'accès au téléservice.

La Commission n'a pas, en l'état, d'observations à formuler sur le dispositif d'authentification par « login » et mot de passe aujourd'hui déployé par le GIP-MDS, sans préjudice des avis ou recommandations qu'elle sera amenée à émettre ultérieurement sur le recours à des dispositifs alternatifs.

À cet égard, la Commission observe qu'une étude est en cours de réalisation par le GIP-MDS visant à la mise en œuvre, dans le cadre du programme net-entreprises, d'un procédé d'authentification des déclarants reposant sur l'émission de certificats électroniques personnels normalisés, projet dans lequel l'utilisation du NIR ne serait pas exclue.

La Commission estime qu'une utilisation du NIR à de telles fins ne peut qu'appeler de sa part une réserve de principe dans la mesure où la concrétisation d'un tel projet constituerait un précédent en faveur de l'utilisation généralisée de cet identifiant particulier dans le cadre de dispositifs de certificats électroniques délivrés aux citoyens souhaitant acheter ou vendre sur internet, voter à distance, consulter leur e-dossier, etc., et aurait pour conséquence la constitution, par les sociétés de certification prestataires, de bases de données contenant les références de plusieurs millions de professionnels ou de leurs délégataires identifiés par leur NIR.

Enfin, la Commission considère que la sécurité du traitement devrait être renforcée sur le plan juridique par l'intégration dans les contrats de prestation de service, au-delà des clauses de confidentialité et de réversibilité déjà introduites, d'une clause de non-détournement de finalité.

Sur *les durées de conservation des données*

Le GIP-MDS assurera une historisation des déclarations sur le site net-DCR sur quatre années afin de permettre aux déclarants d'apporter aisément la preuve du contenu de leur déclaration durant les délais de prescription légaux.

La Commission considère que cette durée n'est pas excessive au regard des finalités poursuivies.

Sur l'information des personnes concernées

L'information des cotisants sera réalisée sur le site www.net-entreprises.fr et notamment sur les pages où la collecte des informations nominatives sera opérée.

La Commission prend acte de ces mesures d'information des personnes concernées.

Émet un avis favorable à la demande d'avis présentée par le GIP-MDS sous réserve que :
— le dispositif de journalisation des connexions existant prévoie une exploitation régulière des données de connexion et un recueil de données sur la nature des opérations effectuées à chaque connexion ;
— une clause de non-détournement de finalité soit intégrée dans le contrat liant le GIP-MDS à l'entreprise assurant l'hébergement du site net-DCR ;

Demande à être rendue destinataire d'un bilan de la mise en œuvre du téléservice dans un délai d'un an.

ANNEXES

Annexe 1

Composition de la CNIL au 1er janvier 2003

Président : **Michel GENTOT,** président de section au Conseil d'État

Vice-président délégué : **Hubert BOUCHET,** membre du Conseil économique et social

Vice-président : **Alex T-RK,** sénateur du Nord

Commissaires :

Cécile ALVERGNAT, consultant et formatrice NTIC

Maurice BENASSAYAG, conseiller d'État

Francis DELATTRE, député du Val-d'Oise

Patrick DELNATTE, député du Nord

Didier GASSE, conseiller-maître à la Cour des comptes

François GIQUEL, conseiller-maître à la Cour des comptes

Pierre LECLERCQ, conseiller honoraire à la Cour de Cassation

Philippe LEMOINE, président-directeur général de Laser, membre du directoire des Galeries Lafayette

Jean-Pierre de LONGEVIALLE, conseiller d'État honoraire

Philippe NOGRIX, sénateur de l'Ille-et-Vilaine

Marcel PINET, conseiller d'État honoraire

Guy ROSIER, conseiller-maître honoraire à la Cour des comptes

Pierre SCHAPIRA, vice-président du Conseil économique et social, adjoint au maire de Paris chargé des relations internationales

Maurice VIENNOIS, conseiller-doyen honoraire à la Cour de Cassation

Commissaires du gouvernement :

Charlotte-Marie PITRAT

Catherine POZZO DI BORGO, adjoint

Annexe 2

Répartition des secteurs d'activité

Hubert BOUCHET, vice-président délégué : emploi, recrutement, formation, élections professionnelles

Alex T-RK, vice-président : coopération européenne et internationale en matière de police, justice et douanes, presse, églises, associations, syndicats

Cécile ALVERGNAT : commerce électronique, plate-forme d'intermédiation, modes de paiement sur internet

Maurice BENASSAYAG : enseignement public et privé, culture, jeunesse et sport, partis politiques, sondages d'opinion, marketing politique, droit d'accès indirect

Francis DELATTRE : santé : établissements de santé, cabinets médicaux, prévention, réseaux de soins, fichiers des professions de santé, sites web médicaux

Patrick DELNATTE : justice (autorités judiciaires, justice administrative, professions judiciaires), autorités administratives indépendantes, Archives nationales

Didier GASSE : marketing, poste, assurance, renseignement commercial, recouvrement de créance, droit d'accès indirect

François GIQUEL : police nationale, gendarmerie nationale, police municipale, renseignement militaire et civil, service national, affaires étrangères, droit d'accès indirect

Pierre LECLERCQ : collectivités locales (hors police municipale, aide sociale, fiscalité locale), recherche médicale, droit d'accès indirect

Philippe LEMOINE : publicité en ligne, télébillétique, localisation des véhicules, veille technologique

Jean-Pierre de LONGEVIALLE : trésor public, fiscalité, cadastre, publicité foncière, douanes, répression des fraudes, comptabilité publique, droit d'accès indirect

Philippe NOGRIX : banque, bourse, crédit à la consommation

Marcel PINET : télécommunications et réseaux, dont internet (notamment fournisseurs d'accès et d'hébergement, diffusion de données publiques sur internet), sécurité, cryptologie, participation aux groupes de travail internationaux dans ce domaine, participation au groupe européen dit de « l'article 29 », droit d'accès indirect

Guy ROSIER : enquêtes statistiques mises en oeuvre par l'INSEE, tourisme, logement, immobilier, transport, équipement, environnement, industrie, énergies, artisanat, agriculture, droit d'accès indirect

Pierre SCHAPIRA : aide sociale, action sociale, revenu minimum d'insertion

Maurice VIENNOIS : sécurité sociale (assurance vieillesse, assurance maladie, allocations familiales) assurance maladie complémentaire, droit d'accès indirect

Annexe 3

Organisation des services au 1er janvier 2003

Président : **Michel GENTOT**
Secrétaire général, chargé des affaires juridiques : **Christophe PALLEZ**

Annexe 4

Liste des délibérations adoptées par la CNIL en 2002

Les délibérations sont publiées dans la deuxième partie du rapport. Elles sont signalées dans le tableau suivant, par un renvoi à la page concordante.

Le texte intégral de l'ensemble des délibérations de la CNIL, depuis 1978, est accessible par internet sur le site http ://www.legifrance.gouv.fr

Numéro Date	Objet
02-001 8 janvier 2002 (*cf.* p. 292)	Délibération concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration (norme simplifiée n° 42)
02-002 24 janvier 2002 (*cf.* p. 273)	Délibération concernant un traitement automatisé de l'INSEE visant à l'exploitation d'informations fiscales pour l'élaboration et la diffusion de produits statistiques locaux sur les revenus des ménages, l'impôt sur le revenu et la taxe d'habitation relative à la résidence principale
02-003 5 février 2002 (*cf.* p. 235)	Délibération portant avis sur un projet de décret fixant les modalités de la transmission de données individuelles prévues à l'article L. 3622-6 du Code de la santé publique et les garanties du respect de l'anonymat des personnes qui s'y attachent
02-004 5 février 2002 (*cf.* p. 296)	Délibération portant adoption du rapport relatif à la cybersurveillance sur les lieux de travail
02-005 5 février 2002 (*cf.* p. 256)	Délibération portant avis sur un projet de décret relatif à l'organisation de l'assurance des non salariés agricoles contre les accidents du travail et les maladies professionnelles
02-006 14 février 2002	Délibération décidant un contrôle sur place
02-007 14 février 2002	Délibération décidant un contrôle sur place

Numéro Date	Objet
02-008 7 mars 2002 (*cf.* p. 201)	Délibération portant avis sur un projet de décret modifiant le Code de procédure pénale et relatif au fichier national des empreintes génétiques
02-009 7 mars 2002 (*cf.* p. 278)	Délibération relative au projet de décret en Conseil d'État portant extension en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, dans les terres australes et antarctiques françaises et à Mayotte du décret n° 78-774 du 17 juillet 1978
02-010 7 mars 2002 (*cf.* p. 185)	Délibération concernant la mise à la disposition des particuliers et des agents des administrations fiscales d'un service de consultation des dossiers fiscaux en ligne et la pérennisation de la procédure de transmission par internet des déclarations annuelles de revenus
02-011 7 mars 2002 (*cf.* p. 279)	Délibération portant avis sur un projet de décret portant application de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'enregistrement et à la conservation d'informations relatives aux actes de l'état civil par les mairies de la collectivité départementale de Mayotte, par le greffe du tribunal de première instance de Mamoudzou, par le secrétariat d'Etat à l'outre-mer ainsi que par la Commission de révision de l'état civil chargée d'établir les actes qui auraient dû être portés sur les registres de l'état civil de droit commun et de droit local de Mayotte
02-012 14 mars 2002 (*cf.* p. 281)	Délibération portant avis sur le projet de décret, présenté par le ministère de l'Économie et des Finances, 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 oeuvre à l'occasion du recensement général de la population (RGP) à Mayotte en 2002
02-013 14 mars 2002 (*cf.* p. 282)	Délibération portant avis sur la mise en œuvre, par le ministère de l'Économie et des Finances, du recensement général de la population (RGP) à Mayotte en 2002
02-014 14 mars 2002 (*cf.* p. 206)	Délibération portant avis sur un projet de décret relatif à l'annuaire universel et modifiant le Code des postes et télécommunications

Numéro Date	Objet
)2-015 14 mars 2002 (*cf.* p. 169]	Délibération portant avis sur un projet d'arrêté présenté par la mairie de Mérignac concernant l'expérimentation d'un dispositif de vote électronique reposant sur l'utilisation de cartes à microprocesseur comportant les empreintes digitales des électeurs
)2-016 21 mars 2002	Délibération décidant un contrôle sur place
)2-017 21 mars 2002 (*cf.* p. 297)	Délibération portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement
)2-018 21 mars 2002 (*cf.* p. 302)	Délibération portant adoption d'un modèle de questionnaire de candidature
)2-019 21 mars 2002	Délibération décidant un contrôle sur place
)2-020 21 mars 2002 (*cf.* p. 238)	Délibération sur un projet d'arrêté relatif à la notification obligatoire des infections aiguës symptomatiques par le virus de l'hépatite B et des infections par le virus de l'immunodéficience humaine
)2-021 2 avril 2002 (*cf.* p. 241)	Délibération sur un projet de décret relatif aux conditions dans lesquelles l'institut de veille sanitaire accède aux informations couvertes par le secret médical et industriel et modifiant le Code de la santé publique
)2-022 2 avril 2002 (*cf.* p. 172)	Délibération relative à la demande d'avis présentée par la mairie de Vandœuvre-lès-Nancy concernant l'expérimentation d'un dispositif de vote électronique par internet à l'occasion de l'élection présidentielle
)2-023 2 avril 2002	Délibération décidant un contrôle sur place
)2-024 23 avril 2002 (*cf.* p. 244)	Délibération relative à la mission de vérification sur place effectuée auprès de la société CEGEDIM

Numéro Date	Objet
02-025 23 avril 2002	Délibération décidant un contrôle sur place
02-026 23 avril 2002	Délibération décidant un contrôle sur place
02-027 23 avril 2002	Délibération décidant un contrôle sur place
02-028 23 avril 2002	Délibération décidant un contrôle sur place
02-029 23 avril 2002	Délibération décidant un contrôle sur place
02-030 23 avril 2002	Délibération décidant un contrôle sur place
02-031 23 avril 2002	Délibération décidant un contrôle sur place
02-032 23 avril 2002	Délibération décidant un contrôle sur place
02-033 23 avril 2002 (*cf.* p. 161)	Délibération relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux
02-034 23 avril 2002 (*cf.* p. 163)	Délibération portant avis sur un projet de décision du directeur général de l'établissement public aéroports de Paris relative à une expérimentation de trois dispositifs biométriques de contrôle des accès aux zones réservées de sûreté des aéroports d'Orly et de Roissy
02-035 23 avril 2002	Délibération décidant un contrôle sur place
02-036 23 avril 2002	Délibération décidant un contrôle sur place

Numéro Date	Objet
02-037 23 avril 2002	Délibération décidant un contrôle sur place
02-038 23 avril 2002	Délibération décidant un contrôle sur place
02-039 23 avril 2002	Délibération décidant un contrôle sur place
02-040 23 avril 2002	Délibération décidant un contrôle sur place
02-041 23 avril 2002	Délibération décidant un contrôle sur place
02-042 23 avril 2002	Délibération décidant un contrôle sur place
02-043 23 mai 2002	Délibération décidant un contrôle sur place
02-044 30 mai 2002 (*cf.* p. 284)	Délibération portant avis sur : — un projet de décret en Conseil d'Etat présenté par le ministère de l'Économie, des Finances et de l'Industrie pris en application de l'article 18 de la loi de 6 janvier 1978 autorisant l'INSEE à utiliser le RNIPP dans le cadre d'études de mortalité réalisées à partir d'échantillon de population ; — la mise en œuvre par l'INSEE d'applications informatiques relatives à des études de mortalité différentielle réalisées à partir de la création d'échantillons de population issus du recensement général de 1999 et du fichier des déclarations annuelles des données sociales
02-045 18 juin 2002 (*cf.* p. 165)	Délibération portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF
02-046 18 juin 2002	Délibération décidant un contrôle sur place

Numéro Date	Objet
02-047 27 juin 2002 (*cf.* p. 259)	Délibération relative au projet de décret présenté par le ministère de l'Intérieur portant modification de l'application de gestion des ressortissants étrangers en France (AGDREF) et à la demande d'avis de la Caisse nationale des allocations familiales relative à l'exploitation de certaines données extraites du fichier AGDREF dans le cadre de son obligation de contrôle de régularité du séjour des personnes étrangères souhaitant bénéficier de prestations familiales
02-048 27 juin 2002 (*cf.* p. 215)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
02-049 27 juin 2002	Délibération décidant un contrôle sur place
02-050 27 juin 2002	Délibération décidant un contrôle sur place
02-051 27 juin 2002	Délibération décidant un contrôle sur place
02-052 27 juin 2002	Délibération décidant un contrôle sur place
02-053 9 juillet 2002 (*cf.* p. 252)	Délibération portant avis sur : — un projet de décret en Conseil d'État présenté par le ministre de l'Économie, des Finances et de l'Industrie pris en application de l'article 18 de la loi du 6 janvier 1978 autorisant l'INSEE à utiliser le numéro d'inscription au répertoire (NIR) pour le traitement automatisé d'informations nominatives relatif à l'établissement de statistiques comparées sur les valeurs de consommation de soins et de biens médicaux ; — la mise en œuvre, par l'INSEE, d'un traitement automatisé d'informations individuelles relatif à une enquête obligatoire sur la santé et la consommation médicale
02-054 9 juillet 2002 (*cf.* p. 218)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

Numéro Date	Objet
02-055 9 juillet 2002 *{ cf.* p. 268)	Délibération relative à un projet de décret portant création de traitements automatisés d'informations nominatives pour assurer d'une part l'instruction des dossiers d'information présentés en application du décret n° 99-778 du 10 septembre 1999 modifié, d'autre part le paiement des indemnisations servies sur la base du présent décret
02-056 9 juillet 2002 (*cf.* p. 271)	Délibération relative à un projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi 78-17 du 6 janvier 1978 aux fichiers mis en oeuvre pour l'application de décret du 10 septembre 1999 modifié instituant une commission pour l'indemnisation des victimes des spoliations intervenues du fait des législations antisémites en vigueur pendant l'Occupation
02-057 17 septembre 2002	Délibération portant élection du vice-président de la Commission nationale de l'informatique et des libertés
02-058 17 septembre 2002 (*cf.* p. 254)	Délibération portant avertissement à l'association hospitalière du bassin de Longwy
02-059 17 septembre 2002	Délibération décidant un contrôle sur place
02-060 17 septembre 2002	Délibération décidant un contrôle sur place
02-061 17 septembre 2002	Délibération décidant un contrôle sur place
02-062 17 septembre 2002	Délibération décidant un contrôle sur place
02-063 17 septembre 2002	Délibération décidant un contrôle sur place
02-064 17 septembre 2002	Délibération décidant un contrôle sur place
02-065 24 septembre 2002 (*cf.* p. 223)	Délibération portant avertissement à la société « Audit et solutions »

Numéro Date	Objet
02-066 24 septembre 2002 (*cf.* p. 195)	Délibération portant avis sur la modification du traitement mis en œuvre dans le cadre du site internet Légifrance
02-067 24 septembre 2002 (*cf.* p. 263)	Délibération portant avis sur la mise en œuvre, par la Croix-Rouge française, d'un traitement d'informations nominatives dont l'objet est d'assurer la délivrance de badges d'accès aux personnes hébergées dans le centre d'accueil de Sangatte
02-068 24 septembre 2002	Délibération décidant un contrôle sur place
02-069 15 octobre 2002 (*cf.* p. 183)	Délibération portant avis sur le projet d'arrêté présenté par le ministère de la Jeunesse, de l'Education nationale et de la Recherche concernant la modification du traitement SCOLARITÉ
02-070 15 octobre 2002 (*cf.* p. 167)	Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Joliot-Curie de Carqueiranne, destiné à contrôler l'accès au restaurant scolaire par la reconnaissance de la géométrie de la main
02-071 15 octobre 2002 (*cf.* p. 212)	Délibération portant avis sur le traitement automatisé d'informations nominatives mis en œuvre par La Poste relatif au fichier des nouveaux voisins
02-072 24 octobre 2002 (*cf.* p. 197)	Délibération portant avis sur le projet d'arrêté du ministère de la Justice abrogeant et remplaçant l'arrêté du 28 octobre 1996 portant création d'un fichier national des personnes incarcérées
02-073 24 octobre 2002 (*cf.* p. 199)	Délibération portant avis sur le projet d'arrêté du ministère de la Justice abrogeant et remplaçant l'arrêté du 4 février 1991 portant création d'un système de gestion automatisée de la prise en charge des détenus dans les établissements pénitentiaires
02-074 24 octobre 2002 (*cf.* p. 224)	Délibération portant adoption du rapport relatif à l'opération « Boîte à Spams »
02-075 24 octobre 2002 (*cf.* p. 225)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978

Numéro Date	Objet
02-076 24 octobre 2002 *(cf.* p. 227)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
02-077 24 octobre 2002 *(cf.* p. 229]	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
02-078 24 octobre 2002 (*cf.* p. 231)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
02-079 24 octobre 2002 *(cf.* p. 233)	Délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978
02-080 15 octobre 2002	Délibération décidant un contrôle sur place
02-081 15 octobre 2002	Délibération décidant un contrôle sur place
02-082 19 novembre 2002 (*cf.* p. 248)	Délibération sur une demande d'autorisation présentée par l'Institut national de veille sanitaire concernant la mise en place de l'application informatique destinée à la surveillance épidémiologique nationale des maladies infectieuses à déclaration obligatoire dont le VIH/sida, et sur un projet d'arrêté présenté par le ministère de la Santé relatif à la notification obligatoire des maladies infectieuses visées à l'article d11-1 du Code de la santé publique
02-083 19 novembre 2002	Délibération décidant un contrôle sur place
02-084 19 novembre 2002	Délibération décidant un contrôle sur place
02-085 19 novembre 2002	Délibération décidant un contrôle sur place
02-086 19 novembre 2002	Délibération décidant un contrôle sur place

Numéro Date	Objet
02-087 19 novembre 2002	Délibération décidant un contrôle sur place
02-088 19 novembre 2002	Délibération décidant un contrôle sur place
02-089 19 novembre 2002	Délibération décidant un contrôle sur place
02-090 28 novembre 2002 (*cf.* p. 174)	Délibération relative à la demande d'avis présentée par la mairie d'Issy-les-Moulineaux concernant l'expérimentation d'un dispositif de vote électronique par internet lors des élections des conseils de quartier
02-091 28 novembre 2002 (*cf.* p. 176)	Délibération relative à la demande d'avis présentée par la mairie d'Issy-les-Moulineaux concernant l'expérimentation d'un dispositif de vote électronique par internet lors des élections prud'homales
02-092 28 novembre 2002 (*cf.* p. 191)	Délibération concernant la modification de plusieurs traitements d'informations nominatives mis en oeuvre par la direction générale des impôts et certains aménagements dans les relations avec les contribuables résultant de l'entrée en vigueur des dispositions fiscales de la loi relative au PACS
02-093 28 novembre 2002 (*cf.* p. 178)	Délibération portant avis sur le projet de loi relatif à l'économie numérique
02-094 10 décembre 2002 (*cf.* p. 266)	Délibération concernant un projet de décret modifiant le décret n° 97-1321 du 30 décembre 1997 relatif aux documents ouvrant droit aux prestations de l'assurance maladie
02-095 10 décembre 2002	Délibération décidant un contrôle sur place
02-096 10 décembre 2002	Délibération décidant un contrôle sur place
02-097 10 décembre 2002	Délibération décidant un contrôle sur place

Numéro Date	Objet
02-098 10 décembre 2002	Délibération décidant un contrôle sur place
02-099 10 décembre 2002	Délibération décidant un contrôle sur place
02-100 10 décembre 2002	Délibération décidant un contrôle sur place
02-101 10 décembre 2002	Délibération décidant un contrôle sur place
02-102 10 décembre 2002	Délibération décidant un contrôle sur place
02-103 10 décembre 2002	Délibération décidant un contrôle sur place
02-104 10 décembre 2002	Délibération décidant un contrôle sur place
02-105 10 décembre 2002	Délibération décidant un contrôle sur place
02-106 19 décembre 2002 (*cf. p.* 307)	Délibération portant avis sur le projet de décret en Conseil d'État pris pour l'application de l'article L. 133-5 du Code de la Sécurité sociale concernant l'utilisation du NIR dans le cadre des télédéclarations effectuées sur le portail www.net-entreprises.fr
02-107 19 décembre 2002 (cf. p. 310)	Délibération relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DUCS-I sur le portail www.net-entreprises.fr
02-108 19 décembre 2002 (cf. p. 314)	Délibération relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DADS-U sur le portail www.net-entreprises.fr

Numéro Date	Objet
02-109 19 décembre 2002 (*cf.* p. 318)	Délibération relative à une demande d'avis présentée par le groupement d'intérêt public « Modernisation des déclarations sociales » pour la mise en œuvre de la télédéclaration Net-DCR sur le portail www.net-entreprises.fr
02-110 19 décembre 2002 (*cf.* p. 159)	Délibération portant avis sur la modification de la loi du 9 juillet 1991 portant réforme des procédures civiles d'exécution visant à permettre aux huissiers d'interroger directement l'administration fiscale détentrice du fichier des comptes bancaires (FICOBA)
02-111 19 décembre 2002 (*cf.* p. 287)	Délibération portant avis sur le projet de décret en Conseil d'État pris pour l'application du titre V de la loi n° 2002-276 du 27 février 2002

Annexe 5

Questions parlementaires

Assemblée nationale

Question n° : 70149 de M. **Jean-Claude Lefort,** ministère interrogé : Industrie
Réponse publiée au JO le 21 janvier 2002 (page 337)

Télécommunications — Internet. Courriers électroniques commerciaux. Réglementation

Question : M. Jean-Claude Lefort attire l'attention de M. le secrétaire d'Etat à l'Industrie sur la régulation nécessaire des courriers électroniques commerciaux non sollicités, pratique plus couramment appelée « spam ». Au rythme où cette pratique se développe, parfois de manière agressive, elle risque en effet de saturer très rapidement la patience des utilisateurs du courrier électronique et de compromettre à moyen terme le développement internet. Cette question est au centre du débat sur une directive européenne relative à la protection de la vie privée, débat dans lequel la France a malheureusement défendu une position favorable aux annonceurs. Cette position, appelée *« op-out »,* consiste à autoriser le « spam » à condition d'offrir la possibilité de faire cesser les envois suivants par retour de courrier. Ce système fait supporter à l'usager le coût du tri des messages et de la connexion. Il est d'autant moins justifiable qu'il existerait une autre solution, appelée *« opt-in »,* qui exigerait d'obtenir l'accord préalable de l'usager avant d'envoyer un message publicitaire, voire de créer des listes d'abonnés refusant de recevoir de la publicité par courrier. Il lui demande pourquoi la France a choisi la première de ces solutions et s'il entend revenir sur ce choix dans la discussion du projet de loi sur la société de l'information.

Réponse : un accord politique a été obtenu lors du Conseil des ministres de l'Union européenne (transports/télécommunications) du 6 décembre 2001 sur la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Il repose sur l'interdiction des communications commerciales non sollicitées, par mél, par télécopie ou par automates d'appels (pollupostage ou « spam »). L'utilisation de ces moyens n'est autorisée que pour les abonnés ayant donné leur consentement préalable *(« opt-in »).* Toutefois, les entreprises qui auront obtenu directement de leurs clients, à l'occasion d'un achat, les données nécessaires à l'octroi d'un message électronique pourront en faire usage pour leur propre prospection commerciale, sauf opposition de l'abonné *(« opt-out »).* Cette position répond aux préoccupations des consommateurs, tout en reconnaissant aux entreprises la capacité de poursuivre une relation avec leurs clients. Elle prévoit, quelle que soit la technologie utilisée, une harmonisation des pratiques en Europe, ce qui confortera le marché intérieur. C'est pourquoi la France a soutenu cette proposition qui sera examinée par le Parlement européen dans le cadre de la seconde lecture au projet de directive. Ces orientations seront prises en compte au niveau national dans le cadre du débat parlementaire sur le projet de loi sur la société de l'information.

Assemblée nationale

Question n° : 69019 de M. **Henri Sicre,** ministère interrogé : Intérieur
Réponse publiée au *JO* le 21 janvier 2002 (page 348)

Police — Police judiciaire. Système de traitement des infractions constatées. Accès

Question : M. Henri Sicre demande à M. le ministre de l'Intérieur qui (et dans quelles conditions) est autorisé à consulter le fichier des antécédents judiciaires, baptisé « Système de traitement des infractions constatées » (STIC).

Réponse : le système de traitement des infractions constatées (STIC) est un fichier de police judiciaire dont la finalité est la rationalisation du recueil et de l'exploitation des informations contenues dans les procédures établies par les services de police, dans le cadre de leur mission de police judiciaire, aux fins de recherches criminelles et de statistiques. Ce fichier a été autorisé par décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le texte réglementaire a reçu l'avis conforme de la CNIL le 19 décembre 2000, un avis favorable du Conseil d'Etat le 19 février 2001 et a été publié au *Journal officiel* du 6 juillet 2001. Aux termes de l'article 5 du décret, les destinataires des données du traitement sont les personnels des services de la police nationale et de la gendarmerie nationale qui exercent des missions de police judiciaire et ont fait l'objet d'une désignation par l'autorité hiérarchique, ainsi que les magistrats du parquet. Dans le cadre de mission de police administrative, la consultation du STIC est, conformément à l'article 6, réservée aux personnels de la police nationale individuellement désignés et spécialement habilités par le directeur général de la police nationale ou par le préfet. L'habilitation comporte deux niveaux d'accès. Elle précise le niveau qui est conféré à son titulaire par l'autorité compétente. Les modalités du droit d'accès des personnes intéressées, précisées à l'article 8, s'exercent d'une manière indirecte, dans les conditions prévues à l'article 39 de la loi du 6 janvier 1978 précitée.

Assemblée nationale

Question n° : *67860* de M. **André Aschieri,** ministère interrogé : Intérieur
Réponse publiée au *JO* le 4 février 2002 (page 592)

Internet — Données personnelles. Mineurs. Protection

Question : M. André Aschieri appelle l'attention de M. le ministre de l'Intérieur sur les inquiétudes formulées par la CNIL concernant la protection des mineurs à l'égard de la collecte de données sur internet. La CNIL préconise que les campagnes d'information audiovisuelles menées sur la protection des mineurs soient élargies à la protection des données personnelles. Il lui demande de lui indiquer les mesures qu'il entend prendre afin de garantir la protection des mineurs.

Réponse : l'arrêté du 8 novembre 2001 portant création du site www.internet-mineurs.gouv.fr, publié au *Journal officiel de la République française* du 9 novembre 2001 (p. 17808), dispose qu'il est créé un site internet public dont la finalité est de permettre aux utilisateurs de l'internet de signaler les sites susceptibles de contrevenir aux lois françaises relatives à la protection des mineurs. À cet effet, une messagerie électronique, contact@signale.internet-mineurs.gouv.fr, permet de signaler tous contenus textuels, graphiques, audiovisuels ou multimédias circulant sur l'internet. Il est créé, à l'Office central de lutte contre la criminalité liée aux technolo-

gies de l'information et de la communication du ministère de l'intérieur, un traitement automatisé d'informations qui a pour objet la mise en place d'une base de données pour le regroupement des signalements précités, en vue de permettre aux services d'enquêtes de disposer de toutes les informations nécessaires aux poursuites susceptibles d'être engagées, ou de tous les renseignements complémentaires utiles aux poursuites déjà engagées, ainsi que de constituer une base de données des signalements en vue de les rapprocher des signalements ultérieurs.

Assemblée nationale

Question n° : 70157 de M. **Bernard Schreiner,** ministère interrogé : Justice
Réponse publiée au *JO* le 18 février 2002 (page 981)

Baux d'habitation — Locataires défaillants. Bailleur. Protection

Question : M. Bernard Schreiner appelle l'attention de M^me^ la garde des Sceaux, ministre de la Justice, sur la nécessité d'instaurer un fichier des locataires défaillants, fichier national qui devrait être accessible aux bailleurs privés et sociaux pour être de quelque utilité. La Banque de France gère déjà deux fichiers de ce type. L'un, le plus ancien, enregistre les émissions de chèques sans provision et les interdits bancaires. L'autre, instauré 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, recense les incidents de paiements caractérisés liés aux crédits accordés aux particuliers. Ces deux fichiers permettent aux établissements financiers d'avoir une meilleure connaissance des capacités financières réelles des candidats emprunteurs et des incidents financiers qu'ils ont pu connaître dans un passé récent. S'agissant des rapports locataires-bailleurs, ces derniers sont particulièrement démunis face à des locataires de mauvaise foi qui, sans être insolvables, s'abstiennent néanmoins volontairement de verser régulièrement les loyers et charges dus. Pendant ce temps, le bailleur est tenu, malgré l'absence de paiement du loyer, de faire l'avance des charges locatives sans pouvoir arguer de la défaillance du preneur. Il est également tenu de verser au percepteur la taxe des ordures ménagères due par le locataire sans être assuré de pouvoir récupérer en fin de compte. D'ailleurs, avec toutes les règles très protectrices des locataires, le bailleur privé est certain d'assurer pendant douze à dix-huit mois au minimum le gîte gratuit au locataire défaillant sans grand espoir de rentrer dans ses frais ni de récupérer totalement sa créance de loyer et de charges. Il y a, manifestement, une rupture d'égalité criante entre les intérêts en présence. Pour rétablir quelque peu l'égalité entre bailleur et locataire, ainsi que la sécurité juridique des bailleurs privés, il lui demande si elle envisage la mise en place d'un fichier recensant les locataires défaillants qui serait fort utile sous réserve toutefois que l'accès à l'information soit ouverte aux bailleurs, éventuellement par l'intermédiaire des ADIL départementales si l'on ne souhaite pas donner accès aux bailleurs privés.

Réponse : la proposition de mise en place d'un fichier des locataires défaillants pose la question de l'adéquation de ce moyen avec l'objectif de lutter contre les locataires de mauvaise foi. En effet, dès lors que les conditions objectives de la résolution du contrat sont réunies, il n'est pas nécessaire au juge de rechercher un élément moral pour prendre sa décision. Les jugements ne permettant donc pas de distinguer les locataires selon leur bonne ou mauvaise foi, le fichier proposé comprendrait nécessairement l'ensemble des décisions constatant la résolution d'un contrat de bail. La comparaison de ce projet de fichier avec ceux des incidents et des interdictions de paiement en matière de chèques, et des incidents de paiement carac-

térisés, prévus par le code monétaire et financier, doit être prudente. En effet, des règles très strictes permettent d'assurer la confidentialité de ces fichiers, alors que la diffusion des informations aux bailleurs, même après filtrage par les ADIL, serait potentiellement beaucoup plus large, ne serait-ce qu'en raison du nombre de ces derniers. Un fichier des locataires défaillants poserait aussi problème au regard de l'article 22-1 de la loi n° 89-462 du 6 juillet 1989 tel que modifié par la loi n° 2002-73 du 17 janvier 2002 de modernisation sociale, qui interdit notamment au bailleur de demander au candidat à la location un relevé de compte bancaire ou une attestation de bonne tenue de compte bancaire ou postal. On pourrait en effet s'interroger sur la cohérence d'une politique législative qui, après avoir prohibé l'accès du bailleur à une information fournie par le candidat preneur sur ses capacités financières, en vue de protéger ce dernier, organiserait la divulgation d'une information sur ses antécédents civils, susceptibles de porter une atteinte bien plus importante à sa vie privée. Il convient par ailleurs de rappeler que l'absence temporaire du paiement d'un loyer n'exonère jamais le preneur de sa dette, et que le fait pour un débiteur d'organiser ou d'aggraver son insolvabilité est réprimé par l'article 314-7 du Code pénal. La solution au problème posé doit être recherchée dans la bonne application de ces règles, et non dans la mise en place d'un dispositif dont les effets sur l'exclusion de locataires précaires et sur la protection de la vie privée pourraient révéler des inconvénients excédant les avantages envisagés par l'honorable parlementaire.

Assemblée nationale

Question n° : 70667 de M. **Francis Hillmeyer,** ministère interrogé : Intérieur
Réponse publiée au *JO* le 1er avril 2002 (page 1807)

État civil — Registres. Utilisation. Maires

Question : M. Francis Hillmeyer attire l'attention de M. le ministre de l'Intérieur sur les civilités d'usage que le maire doit à ses administrés. Le quotidien des habitants d'une commune est ponctué par un certain nombre d'événements familiaux, tantôt heureux, tantôt sombres. L'on se réjouit dans tel foyer d'une naissance, tel administré convole en justes noces, telle famille est endeuillée, etc. En ces circonstances, il est de bon ton que le maire de la commune présente aux personnes concernées ses civilités (compliments, félicitations, condoléances, vœux, etc.) Cette pratique ponctuelle est appréciée par les administrés et, somme toute, normale. Le maire est informé de ces événements familiaux par le biais des différentes déclarations faites à l'état civil en mairie. Or, la Commission nationale de l'informatique et des libertés (CNIL) vient récemment d'émettre à nouveau un avis défavorable quant à l'utilisation par les maires des registres de l'état civil à des fins de communication personnalisée, avis défavorable qui constitue une interdiction implicite. L'on ne peut que s'étonner de cette position compte tenu que ces civilités ne portent en aucun cas atteinte au respect de la vie privée ni à la tranquillité des personnes, mais qu'elle supprime un usage, une tradition séculaire. Il lui demande en conséquence s'il compte prendre des dispositions pour lever cette interdiction implicite de la CNIL.

Réponse : l'utilisation par les maires des registres d'état civil de leurs communes pour l'envoi de courriers personnalisés à l'occasion d'une naissance, d'un décès ou d'un mariage participe d'une action de communication municipale. Dans sa délibération n° 99-24 du 8 avril 1999 portant sur un projet d'arrêté concernant l'envoi de courriers personnalisés aux administrés lors d'événements tels que les décès, naissances et mariages, la Commission nationale de l'informatique et des libertés a considéré que le *« respect du principe de finalité des traitements s'oppose,*

de manière générale, à ce que des informations enregistrées dans un fichier soient utilisées à des fins étrangères à celles qui ont justifié leur collecte et leur traitement ». De plus, la Commission estime *« de doctrine constante, que ce principe de finalité constitue une garantie essentielle au respect de la vie privée et de la tranquillité des personnes, tout particulièrement lorsque des fichiers publics sont en cause »,* ce d'autant que les personnes concernées ne disposent pas de la faculté de s'opposer à y figurer. Dès lors, les données recueillies à l'occasion de cette mission ne sauraient être utilisées à d'autres fins par quiconque, et par conséquent, à des actions de communication municipale.

Assemblée nationale

Question n° : 449 de M^me^ **Marie-Jo Zimmermann,** ministère interrogé : Intérieur Réponse publiée au *JO* le 2 septembre 2002 (page 2999)

Élections et référendums — Elections législatives. Candidats. Réglementation

Question : M^me^ Marie-Jo Zimmermann attire l'attention de M. le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales sur le fait que les circulaires ministérielles enjoignent aux préfectures de demander l'étiquette politique des candidats aux élections législatives. Or, cette notion d'étiquette politique, qui n'a rien à voir avec le parti politique de rattachement pour les aides financières de l'État, ne figure nulle part, ni dans les lois ni dans les décrets. Elle souhaiterait donc qu'il lui indique s'il n'estime pas abusif de demander aux candidats des renseignements qui ne sont pas prévus par la réglementation.

Réponse : la communication par les candidats de leur étiquette aux services préfectoraux à l'occasion de leur déclaration de candidature aux élections législatives des 9 et 16 juin 2002 est prévue par le décret n° 2001-777 du 30 août 2001 portant création d'un fichier unique des candidats aux élections au suffrage universel, décret en Conseil d'Etat pris sur avis conforme de la CNIL. Son article 3 dispose en effet que « *les catégories d'information nominatives enregistrées* [...] *sont les suivantes : […] étiquette politique choisie par le candidat* ». De plus, la communication de l'étiquette présente d'autant moins le caractère d'un acte « abusif » comme l'écrit l'honorable parlementaire qu'elle n'est pas obligatoire, les candidats conservant la faculté de n'en déclarer aucune. Elle n'a pour objet que de permettre l'information des électeurs sur l'appartenance politique des candidats. L'étiquette communiquée par les candidats n'a donc eu d'autre destination qu'une transmission à la presse et aux citoyens, par le biais notamment du site internet du ministère de l'Intérieur. En outre, l'étiquette a pu être modifiée par les candidats à tout moment, même la veille du premier tour ou entre les deux tours s'ils le souhaitaient, et ce sans aucun droit de regard de l'administration.

Assemblée nationale

Question n° : 1182 de M. **Bruno Bourg-Broc,** ministère interrogé : Justice Réponse publiée au *JO* le 4 novembre 2002 (page 4061)

Droits de l'homme et libertés publiques — CNIL. Fichiers informatisés. Contrôle. Réglementation

Question : M. Bruno Bourg-Broc demande à M. le garde des Sceaux, ministre de la Justice, de lui préciser la suite qu'il envisage de réserver à la délibération

n° 2001-057 du 29 novembre 2001 de la Commission nationale de l'informatique et des libertés (CNIL), s'inquiétant de la présence d'informations nominatives relatives à des personnes parties prenantes aux procès et à des témoins dans les bases de données juridiques, toujours plus nombreuses et plus importantes.

Réponse : le garde des Sceaux a l'honneur de faire savoir à l'honorable parlementaire que le développement récent des nouvelles technologies, et en particulier d'internet, nécessite une nouvelle réflexion sur la transmission de l'information et la protection de la vie privée. C'est dans ce cadre que s'inscrit la délibération n° 01-057 du 29 novembre 2001 de la CNIL portant recommandation sur la diffusion de données personnelles sur internet par des banques de données de jurisprudence. Le garde des Sceaux, comme l'a rappelée la CNIL dans sa recommandation précitée, souhaite faire savoir à l'honorable parlementaire qu'il est favorable à un équilibre permettant d'assurer le bon usage des banques de données de jurisprudence qui constituent un outil indispensable pour tous les professionnels du droit, tout en préservant sur internet l'anonymat nécessaire des personnes citées dans les décisions de justice rendues. À ce titre, comme l'a rappelé la CNIL aux éditeurs de base de données des décisions de justice accessibles sur internet ou disponibles sur CD-Rom, ces bases de données constituent, si elles comportent le nom des parties, des traitements automatisés de données nominatives qui doivent faire l'objet d'une déclaration préalable auprès de la CNIL et répondre aux prescriptions des dispositions de la loi du 6 janvier 1978. De ce fait, plusieurs dispositions de la loi du 6 janvier 1978 permettent d'assurer cet équilibre entre la transmission de la connaissance et la protection de la vie privée. Ainsi, les dispositions de l'article 26 de la loi précitée, et qui ont vocation à s'appliquer aux banques de données de jurisprudence, permettent à toute personne de s'opposer, pour des raisons légitimes, à ce que les informations la concernant fassent l'objet d'un traitement automatisé. Il pourra en être ainsi de décisions de justice qui ont fait l'objet d'une mesure d'amnistie, dans la mesure où les dispositions de l'article 133-11 du Code pénal proscrivent le rappel de l'existence de décisions amnistiées. De même, l'article 31 de la loi du 6 janvier 1978 subordonne-t-il la mise en mémoire informatisée de certaines informations qui font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes, au recueil de l'accord express de l'intéressé, sauf autorisation par décret en Conseil d'Etat pris après avis de la CNIL pour un motif d'intérêt public. Or les jugements ou arrêts sont susceptibles de comporter des informations de cette nature lorsqu'elles sont intrinsèquement liées à l'instance en cause. En outre, la diffusion sur internet, sous une forme nominative de jugements ou arrêts non définitifs, peut conduire les personnes concernées à demander la rectification ou l'effacement d'informations les concernant, au motif que la décision a été réformée ou cassée, sur le fondement de l'article 36 de la loi du 6 janvier 1978. Il appartient donc aux éditeurs de respecter les prescriptions émises par la CNIL dans son avis du 29 novembre 2001, sous peine d'être sanctionnés, et le garde des Sceaux, particulièrement vigilant dans ce domaine touchant aux libertés individuelles, ne peut que les encourager à suivre les préconisations de la CNIL tendant à anonymiser les noms des parties et témoins à un procès lorsque ceux-ci sont repris dans le cadre de la mise en ligne de la décision judiciaire. Enfin, dans le cadre d'une réflexion plus globale, le garde des Sceaux entend faire connaître à l'honorable parlementaire que les différents ministères concernés travaillent activement à la préparation de divers textes sur l'économie numérique et l'accès aux données et archives publiques par les réseaux de communication qui auront pour objet, entre autres finalités, de garantir la protection des informations nominatives.

Assemblée nationale

Question n° : 124 de M. **Francis Hillmeyer,** ministère interrogé : Premier ministre
Réponse publiée au *JO* le 18 novembre 2002 (page 4270)

Décorations, insignes et emblèmes — Légion d'honneur. Liste nominative. Contenu

Question : M. Francis Hillmeyer attire l'attention de M. le Premier ministre sur la publication au *Journal officiel* de la liste des personnes élevées, promues ou nommées dans l'ordre national de la Légion d'honneur. Pour chaque personne, il est fait état de son nom (ainsi que du nom de jeune fille pour les dames), de son ou ses prénoms, de sa profession et/ou de ses fonctions (éventuellement aussi du dernier grade dans l'ordre et de la date de nomination), mais aucune mention quant à son domicile. Or, une mention supplémentaire indiquant le lieu de résidence du récipiendaire, sa ville ou sa commune et son département (sans pour autant indiquer son adresse complète afin de préserver sa vie privée), faciliterait grandement la lecture de cette liste, notamment pour les journalistes qui ont évidemment à cœur d'informer rapidement leurs lecteurs de ces nominations de personnalités connues nationalement ou localement, mais aussi pour les élus, parlementaires, élus locaux, etc. qui souhaitent être parmi les premiers à féliciter les dignitaires. Il lui demande quel est son avis eu égard à cette suggestion.

Réponse : le Premier ministre est en mesure de faire savoir à l'honorable parlementaire que la Commission nationale de l'informatique et des libertés, consultée avant la création du fichier informatisé des décorés, avait recommandé d'éviter toute publication d'informations relatives à l'adresse ou au lieu de résidence des membres de la Légion d'honneur. En outre, il a été constaté, depuis quelques années, que certaines personnalités décorées de la Légion d'honneur, identifiées au *Journal officiel en* raison de leur notoriété ou de leurs fonctions, faisaient l'objet, dès la publication du décret, de démarchages commerciaux, voire de sollicitations financières suscitant le plus souvent de la plupart d'entre elles incompréhension ou interrogations. La publication du département d'origine ou de la commune de résidence des personnes nommées ou promues risquerait de faciliter et de généraliser ces pratiques, que la grande chancellerie de la Légion d'honneur s'emploie à combattre. Aussi, le Premier ministre, après examen de la suggestion avancée par l'honorable parlementaire, n'entend-t-il pas modifier la pratique actuellement suivie en la matière.

Sénat

Question n° : 02360 de M. **Serge Mathieu,** ministère interrogé : Justice
Réponse publiée au *JO* le 28 novembre 2002 (page 2889)

Accès *au crédit*

Question : M. Serge Mathieu demande à M. le garde des Sceaux, ministre de la Justice, les perspectives de son action ministérielle à l'égard d'un récent arrêt du Conseil d'État, annulant une recommandation de la CNIL (Commission nationale de l'informatique et des libertés) qui avait mis en garde contre des pratiques bancaires prenant en compte la nationalité dans l'octroi d'un crédit et excluant systématiquement certaines catégories d'étrangers « qualifiés de statistiquement risqués » (Union fédérale des consommateurs. Que Choisir n° 300, février 2002).

Réponse : le garde des Sceaux, ministre de la Justice, fait connaître à l'honorable parlementaire que, par délibérations du 8 juillet 1980 et du 5 juillet 1988, la CNIL s'est prononcée sur la méthode de calcul statistique dite du score *(cré-*

dit scoring), qui constitue pour les établissements de crédit un instrument d'aide à la décision leur permettant d'évaluer, en considération d'une pluralité de paramètres, les risques liés à l'octroi d'un prêt. L'arrêt rendu par le Conseil d'État le 30 octobre 2001 a annulé une nouvelle délibération de la CNIL en date du 22 décembre 1998, par laquelle celle-ci, à la suite de contrôles effectués dans différents établissements de crédit, modifiait sa recommandation du 5 juillet 1988, par l'insertion de deux alinéas additionnels, en décidant notamment que la nationalité du demandeur ne peut constituer une variable entrant en ligne de compte dans le calcul automatisé de l'appréciation du risque du crédit, qu'elle soit considérée sous la forme « Français, ressortissant CEE, autres » ou a *fortiori* enregistrée en tant que telle. Le Conseil d'État a en effet estimé que la nationalité constituait en l'espèce, au regard de la finalité du traitement, une donnée pertinente, adéquate et non excessive, ce, conformément à l'article 5 de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel signée à Strasbourg le 28 janvier 1981, et étant observé que la mise en oeuvre d'un tel critère n'entraîne pas le rejet d'une demande sans examen individuel de celle-ci. Le juge administratif a par ailleurs estimé qu'une telle donnée ne pouvait être qualifiée de discrimination, ni au sens de l'article 6 du traité CE, devenu, après modification, l'article 12 CE, ni au sens des articles 225-1 et 225-2 du Code pénal. Sur ce dernier point, les conclusions du commissaire du Gouvernement soulignent l'absence de volonté discriminatoire tenant au fait que les établissements de crédit contrôlés n'utilisent pas la nationalité précise du candidat au prêt comme variable du score et qu'ils ne s'intéressent à la nationalité qu'eu égard à sa corrélation avec d'éventuelles difficultés ultérieures de recouvrement. Il apparaît au total que l'annulation résultant de l'arrêt du Conseil d'Etat du 30 octobre 2001 n'a pas pour effet de créer un vide juridique ou de nuire à l'effectivité des textes, dans la mesure où elle ne fait pas obstacle à l'application au *crédit scoring* des garanties édictées par la CNIL en cette matière antérieurement à sa recommandation du 22 décembre 1998, conformément à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Toutefois, en réponse aux préoccupations de l'honorable parlementaire, il doit être souligné que le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi susvisée, actuellement soumis au Parlement, dotera la CNIL d'instruments de contrôle plus poussés à l'égard des traitements relevant de la mise en œuvre de la technique du score.

Sénat

Question n° : 01320 de M. **Paul Girod,** ministère interrogé : Santé Réponse publiée au *JO* le 5 décembre 2002 (page 3000)

Sites internet sur la santé et préservation du secret médical

Question : M. Paul Girod appelle l'attention de M. le ministre de la Santé, de la Famille et des Personnes handicapées sur les résultats de l'enquête de la Commission nationale de l'informatique et des libertés (CNIL) par un audit sur cinquante-neuf sites consacrés à la santé et destinés au grand public ou aux professionnels de la santé. La CNIL constate que la législation sur les données personnelles est mal appliquée, notamment, pour chaque internaute entre l'usage interne ou la communication à des tiers. La CNIL recommande que la loi interdise désormais, expressément, la commercialisation de telles données *(Le Particulier,* n° 942, avril 2001). Il lui demande de lui préciser la suite qu'il envisage de réserver à ces observations pour une meilleure protection du secret médical.

Réponse : suite au constat par la CNIL de la mauvaise application de la législation sur les données personnelles faite par les sites internet « santé » et en réponse à son souhait de voir interdire toute commercialisation des données individuelles de santé, deux réponses ont été apportées. D'une part, l'article 11 de la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (créant l'article L. 1111-8 du Code de la santé publique) introduit un nouveau dispositif relatif aux « hébergeurs de données de santé à caractère personnel » encadrant l'utilisation de ces données : « *Les hébergeurs tiennent les données de santé à caractère personnel qui ont été déposées auprès d'eux à la disposition de ceux qui les leur ont confiées. Ils ne peuvent les utiliser à d'autres fins. Ils ne peuvent les transmettre à d'autres personnes que les professionnels de santé ou établissements de santé désignés dans le contrat prévu au deuxième alinéa ».* S'agissant du principe de non-commercialisation de données personnelles de santé, cet article le pose *de facto* dans la mesure où les sites Internet qui recueillent des données personnelles sont des « hébergeurs de données ». Seuls les professionnels identifiés au préalable par contrat pourront accéder aux données déposées par un internaute. Il est précisé que, pour les données se trouvant sur le poste du professionnel, des dispositions législatives existantes interdisent déjà toute commercialisation des données de santé à caractère personnel. D'autre part, le ministère, sensible à la qualité des informations de santé diffusées sur internet, a lancé dès le printemps 2000, en collaboration avec les ordres professionnels et plus particulièrement avec l'ordre national des médecins, le projet « qualité des sites e-santé ». Ce projet a notamment pour objectifs de dégager un référentiel qualité qui permettra à l'internaute de se faire lui-même une opinion sur la qualité des sites internet qu'il consulte et d'assurer à l'usager que les sites qui se réclament de ces règles les respectent bien.

Annexe 6

Protection des données en Europe et dans le monde

L'EXTENSION DE LA PROTECTION EN EUROPE ET DANS LE MONDE

Comme les précédents rapports de la CNIL l'évoquaient déjà, la progression de la protection des données personnelles dans le monde est continue, et, de manière évidente, le modèle européen est le plus repris par les pays adoptant de nouvelles législations en cette matière.

Ainsi, des législations générales de protection des données personnelles, c'est-à-dire des règles applicables à tous les secteurs (publics et privés, notamment) ont été adoptées ou sont rentrées en vigueur dans cinq pays au- cours de l'année 2002, confirmant ce mouvement général d'extension de la protection ainsi que, plus particulièrement, la maturité du droit européen en cette matière.

L'on peut mentionner tout d'abord les pays d'Europe du sud, **Chypre** dont la législation est entrée en vigueur début 2002, ainsi que **Malte,** dont la loi a été votée le 22 mars 2002. Ainsi, les dix États dont l'accession à l'Union européenne est prévue pour 2004 ont d'ores et déjà adopté une législation générale. Deux pays d'Europe centrale et orientale dont l'accession à l'Union européenne est prévue ultérieurement ont également adopté des législations générales en 2002, **la Bulgarie et la Roumanie.** Par ailleurs, le **Liechtenstein,** pays de l'Espace économique européen (EEE) s'est doté d'une législation fondée sur la directive 95/46 CE, et dispose ainsi depuis le 14 mars 2002 d'une loi générale de protection des données personnelles.

Hors d'Europe, de nouvelles initiatives confirment ce mouvement d'extension inexorable de la protection, et plus particulièrement sur le modèle européen de législation générale. Ainsi, en Afrique, le ministère de la Promotion des droits humains du Burkina Faso qui a souhaité que la CNIL effectue une mission en janvier 2003, a annoncé officiellement la préparation d'un avant-projet de loi visant a protection des personnes physiques en matière de traitement des données à caractère personnel.

Des initiatives de législations sectorielles sont également remarquées hors d'Europe. Ainsi, toujours en Afrique, **le législateur sud-africain** a adopté, le 2 août 2002, une loi relative aux communications et transactions électroniques *(Electronic Communications and Transactions Act)* abordant, au sein de nombreux autres sujets, la question de la protection des informations personnelles des individus et retenant un certain nombre de principes relatifs aux conditions de collecte de données personnelles par voie électronique (par exemple, principe de légitimité du traitement, principe de finalité, durées de conservation, etc.).

En Asie, les initiatives doivent être relevées en **Corée du sud,** où la loi relative à la protection des données personnelles sur internet est entrée en vigueur début 2002. Au Japon, plusieurs projets de loi visant le secteur privé et le secteur public, déposés au Parlement en 2001, font l'objet de débats mais n'ont pas encore été adoptés.

Aux Etats-Unis, le débat public national s'est concentré en 2002 sur les projets de l'administration visant à restreindre la liberté de circulation aérienne. En ce qui concerne le secteur privé, de manière sectorielle, diverses initiatives ont vu le jour au niveau des États et au niveau fédéral. Ainsi, dans certains États (Dakota du nord) la technique du référendum a été utilisée pour imposer aux banques de recueillir le

consentement de leurs clients avant de transmettre des données à des filiales d'un même groupe ou à des tiers. Au plan fédéral, la *Federal Trade Commission* a annoncé officiellement dans le cadre de la révision des règles encadrant les activités de télémarketing, l'institution d'un registre dit *« Do-Not-Call List »,* sur lesquels pourront s'inscrire les personnes ne voulant plus être démarchées par téléphone et que les opérateurs de télémarketing auront l'obligation de consulter. Ce système, très critiqué par les opérateurs, correspond à une demande des consommateurs américains d'une meilleure protection de leur vie privée qui a été, semble-t-il, bien entendue par les autorités américaines. Cette liste d'opposition sera mise en place courant 2003.

LE PANORAMA DES LEGISLATIONS

Le panorama des législations adoptées dans le monde est présenté ci après en se fondant sur le niveau des garanties qu'elles présentent au regard de la législation européenne :

— les législations des pays de l'Union européenne, offrant tous un niveau de protection équivalent, du fait, notamment, de la mise en oeuvre de la directive 95/46/CE ;

— les législations des pays de l'Espace économique européen qui, ayant transposé dans leur droit interne la directive 95/46/CE, doivent également être considérés comme accordant un niveau de protection équivalent à celui accordé par les pays membres de l'Union européenn[1] ;

— les dix pays d'Europe centrale et orientale (dits « PECO ») et les pays d'Europe du sud qui accéderont à l'Union européenne en 2004, et qui disposent d'ores et déjà d'une législation générale de protection des données personnelles ;

— les pays dits « tiers », c'est-à-dire non membres de l'Union européenne, ayant fait l'objet d'une décision de la Commission européenne relative à la constatation du caractère adéquat de la protection des données dans ces pays. Mise à part la décision ancienne concernant la Hongrie (citée en tant que pays d'Europe centrale et orientale), trois décisions formelles de reconnaissance d'adéquation ont été adoptées par la Commission européenne ;

— les pays tiers ne rentrant dans aucune des catégories précédemment énoncées mais qui disposent toutefois de législations de protection des données personnelles générales ou sectorielles. Il convient de préciser que des procédures ont été engagées en 2002 tendant à faire reconnaître comme adéquats les niveaux de protection accordés par l'Argentine et Guernesey. Ces décisions sont attendues en 2003. Des consultations ont été également engagées avec la Nouvelle-Zélande et l'Australie mais les lois de protection des données de ce dernier État n'assurent pas, en l'état, la protection des étrangers.

Enfin, ce panorama est complété de la liste des organisations internationales et des instruments internationaux qui régissent la matière.

[1] L'Espace économique européen, ou « EEE » (en anglais, *« European Economie Area »,* abrégé en « EEA ») a été créé en 1992 par accord entre l'Union européenne et l'AELE (« Association européenne de libre échange » ; en anglais, *« European Free Trade Association* », ou « EFTA »). Cet accord ne concerne que trois sur quatre des pays de l'AELE, à savoir l'Islande, la Norvège et le Liechtenstein, à l'exception de la Suisse, qui a rejeté l'EEE par référendum en 1992. Les pays de l'EEE se sont engagés à transposer dans leurs législations nationales environ 1 400 textes communautaires. ^ ce titre, l'Islande, la Norvège et le Liechtenstein ont transposé la directive 95/46/CE dans leur droit interne.

1 — L'Union européenne

Pays	Législation	Autorité de contrôle
Allemagne	♦ Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données, modifiée par la loi fédérale de protection des données du 20 décembre 1990 et amendée par la loi du 14 septembre 1994 ♦ Législations dans les *L□nder* ♦ Loi fédérale de protection des données -2001 *[Bundesdatenschutzgesetz[bKG)).* Disponible en allemand, anglais et français sur le site web	Der Bundesbeauftragte für den Datenschutz (autorité fédérale) Friedrich Ebert Strasse 1 53173 Bonn Allemagne Site web : www.datenschutz.de
Autriche	♦ Loi fédérale sur la protection des données du 18 octobre 1978, amendée en 1986 ♦ Loi de protection des données -2000 (Dotenschufegesetz 2000 (DSG 2000). Disponible en allemand et en anglais sur le site web	Direktor Buro der Datenschutzkommission und des Datenschutzrater Bundeskanzlerant Ballhausplatz 1 1014 Vienne Autriche Site web : www.bka.gv.at/datenschutz
Belgique	♦ Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 ♦ Version coordonnée de la loi relative à la protection des données à caractère personnel du 8 décembre 1992 (11 décembre 1998) ♦ Arrêté royal du 13 mars 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection des données personnelles ♦ Loi du 24 février 2003 sur le statut de l'autorité de protection des données	Commission de la protection de la vie privée Ministère de la Justice Boulevard de Waterloo 115 1000 Bruxelles Site web : http://www.privacy.fgov.be/
Danemark	♦ Loi n" 293 du 8 juin 1978 sur les registres privés et loi n' 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991 ♦ Loi n° 429, relative au traitement des données personnelles — 2000 (Lov nr. 429 af 31. mai 2000 som aendret ved lov nr. 280 af 25. ap). Disponible en anglais sur le site	Datatilsynet Christians Brygge 28 4 sal 1559 Copenhague Danemark Site web : www.datatilsynet.dk
Espagne	♦ Loi du 29 octobre 1992 réglementant le traitement automatisé de données personnelles ♦ Loi organique de protection des données à caractère personnel -1999 *(Ley Orgonica 15/99 de Protection de Datos de Car□cter Personal.* Disponible en anglais sur le site	Agencia de Protection de Datos C/Sagasta, 22 Madrid 28004 Espagne Site web: www.agenciaprotecciondatos.org/
Finlande	♦ Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police ♦ Loi de protection des données personnelles — 1999 (*Persomppgiftslag 22* avril 1999/523). Disponible en anglais sur le site web	Office of the Data Protection Ombudsman Albertïnkatu 25 PO Box 315 00181 Helsinki Finlande Site web : www.tiefosuoja.fi/mdex.htm

Pays	Législation	Autorité de contrôle
France	♦ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ♦ Transposition directive 95/46/CE : projet de loi adopté en première lecture par l'Assemblée nationale le 30 janvier 2002 et au Sénat le 1er avril 2003 (Cf.http://ameli.senat.fr/publication_pl/2001-2002/203.html	Commission nationale de l'informatique et des libertés 21, rue Saint-Guillaume 75340 Paris cedex 07 Site web : www.cnil.fr
Grèce	♦ Loi n° 2472 sur la protection des personnes à l'égard du traitement des données à caractère personnel — 1997	Commission pour la protection des données Omirou 8 PC 10564 Athènes Grèce Site web: www.dpa.gr
Irlande	♦ Loi sur la protection des données du 13 juillet 1988 Loi adoptée le 18 février 2002 (European Communities Data Protection Régulations, 200) (Entrée en vigueur en avril 2002)	Data protection commissioner Block 4, Irish Life Centre Talbot Stree — Dublin 1 Irlande Site web : www.dataprivacy.ie
Italie	♦ Loi n° 675 sur la protection des données personnelles -1996 (modifiée par plusieurs décrets législatifs de 1997,1998 et 1999) (Legge n. 675 del 31 dicembre 1996 — Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) Disponible en anglais sur le site web.	Garante per la protezione dei dati personali Piazza di Monte Citorio n. 121 00186 Rome Italie Site web : www.garanteprivacy.it/ garante/navig/jsp/index. jsp
Luxembourg	♦ Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, amendée en 1992 ♦ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, disponible en allemand et en anglais sur le site web.	Commission nationale pour la protection des données 68, rue de Luxembourg 4221 Esch-sur-Alzette Luxembourg Site web : http://www.cnpd.lu/
Pays-Bas	♦ Loi du 28 décembre 1988 sur la protection des données, complétée par une loi du 21 juin 1990 sur les fichiers de police ♦ Loi de protection des données — 2001 (Wet bescherming persoonsgegevens (WBP) 2001). Disponible en anglais sur le site web	Data Protection Authority Prins Clauslaan 20 Postbus 93374 -2509 AJ. S'Gravenhage Pays-Bas Site web : www.cbpweb.nl
Portugal	♦ Loi no 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 ♦ Loi n" 67/98 relative à la protection des données à caractère personnel — 1998 (Lei da pmtecçao de dados pessoais n° 67/98). Disponible en français et anglais sur le site web	Comissào Nacional de Protecçào de Dados Informatizados 148, rue de Sao Bento 1200 Lisbonne Portugal Site web : www.cnpd.pt
Royaume-Uni	♦ Loi sur la protection des données du 12 juillet 1988 ♦ Loi de protection des données — 1998 (Data Protection Act 19981 Disponible en anglais sur le site web	The office of information Commissioner Wycliffe House — Water Lane Wilmslow — Cheshire SK9 5AF Royaume Uni Site web : www.dataprotedion.gov.uk
Suède	♦ Loi du 11 mai 1973 sur la protection des données ♦ Loi n° 98/204 sur la protection des données — 1998 (Personuppgiftslagen 1998:204). Disponible en anglais sur le site web	Datainspektionen Box 8114 104 20 Stockholm Suède Site web : www.datainspektionen.se

2 — Les pays de l'EEE (Espace économique européen)

Pays	Législation	Autorité de contrôle
Islande	♦ Loi n° 63-1981 relative l'enregistrement de données personnelles— 1981 (Amendée en 1989) Loi n° 77 du 23 mai 2000	Personuvernd Rauôararstig 10 105 Reykjavik Iceland Site web : www.personuvernd.is
Liechtenstein	♦ Loi sur la protection des données *(Datensdwtzgesetzj* du 14 mars 2002	Data Protection Commissioner of the Principality of Liechtenstein Herrengasse 8 9490 Vaduz-Liechtenstein
Norvège	♦ Loi sur les registres de données personnelles — 1978 ♦ Loi du 14 avril 2000	Datatilsynet Postboks8177Dep0034 Oslo 1 Norvège Site web : www.datatilsynet.no

3 — Les pays d'Europe centrale et orientale (PECO) et les pays d'Europe du Sud dont l'accession à l'Union européenne est prévue en 2004

Pays	Législation	Autorités de contrôle/contacts
Chypre	♦ Loi n° 138 (1) 2001 sur le traitement des données personnelles (protection des individus) — 2001	Commission for Personal Data Protection 40 ThDervis Street 1066 Nicosia Cyprus
Estonie	♦ Loi sur la protection des données personnelles — 1997	Estonian Data Protection Inspektorate Pikk 61 15 065 Tallinn Estonia Site web : www.dp.gov.ee
Hongrie	♦ 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 Hongrie Site web : www.obh.hu
Lettonie	♦ Loi sur la protection des données — avril 2000	Ministry of Justice of the Republic of Latvia Department of European Affairs Brivibas boulevard 36 Riga, LV 1050 Latvia
Lituanie	♦ Loi sur la protection des données personnelles — 1996 Amendée en 2000	State Data Protection Inspectorate Gedimino ave.27/2 LT-2600 Vilnius Lithuania Site Web: www.is.lt/dsinsp
Malte	♦ Loi de protection des données personnelles — 2002	Office of the Commissioner for Data Protection Commissioner for Data Protection 280, Republic Street Valletta GPO 01 Malta

Pays	Législation	Autorités de contrôle/contacts
Pologne	♦ Loi sur la protection des données personnelles — 1997	Biuro Geneeralnego Inspektora Powstancow Warszawyl 00-030 Warszawa Poland Site web : www.giodo.gov.pl
République Tchèque	♦ Loi relative à la protection des données personnelles des systèmes informatisés -1992 Loi n° 101/2000 sur la protection des données personnelles — 1er juin 2000	Office for Personal Data Protection Havelkova 22, 13000 Praha 3 Czech Republic Site web : www.uoou.cz
Slovaquie	♦ Loi relative à la protection des données personnelles des systèmes informatisés — 1998	Office for the Protection of Personal Data Urad Vlady SR Namestie Slobody 1 81370 Bratislava 1 Slovak Republic
Slovénie	♦ Loi n° 210-01/89-3 sur la protection des données — 1999	Namestnik varuha clovekovih pravic **Urad** varuha clovekovih pravic Dunajska 56 1000 Ljubljana Slovénie

4 — Les autres pays tiers dont le niveau de protection est adéquat (article 25 de la directive 95/46/CE)

Pays	Législation et autres textes	Décision d'adéquation de la Commission européenne	Autorités de contrôle/contacts
Canada (niveau fédéral)	♦ Loi fédérale sur la protection des renseignements personnels — 1982 ♦ Loi fédérale sur la protection des renseignements personnels et les documents électroniques — 2000	Décision n° 2002/2/CE du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques	Federal privacy commission Tower B, 3rd Floor, 112 Kent Sireet — Otawa, Ontario K1A 1H3 Canada Site web : www.privcom.gc.ca
États-Unis *(Safe Harbor* uniquement)	♦ Principes internationaux de protection des données au sein du *Safe Harbor*	Décision n° 2000/520/CE du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique	Fédéral Trade Commission FTC 600 Pennsylvanie Avenue NW DC 25080 Washington USA

Pays	Législation et autres textes	Décision d'adéquation de la Commission européenne	Autorités de contrôle/contacts
Suisse	♦ Loi fédérale sur la protection des données -1992	Décision no 2000/518/CE du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse	Commissaire à la protection des données Feldeggweg 1 CH-3003 Berne Suisse Site web : www.edsb.ch

5 — Les autres pays tiers ayant adopté une législation

Pays	Législation	Autorité de contrôle
Monaco	♦ Loi n° 1165 relative aux traitements d'informations nominatives — 1993	Commission de contrôle des informations nominatives Gildor Pastor Center, 7, rue du Gablan Bloc B-Bureau 409 98000 Monaco
Nouvelle-Zélande	♦ Loi sur l'information du secteur public — 17 décembre 1982 ♦ Loi sur la vie privée — 1993	Privacy commission PO Box 466 Auckland Nouvelle-Zélande Site web : www.privacy.org.nz
Paraguay	♦ Loi sur la protection des données — 28 décembre 2000	
République de Macédoine	♦ Loi sur la protection des données personnelles — 1994	
Roumanie	♦ Loi relative à la protection des données à caractère personnel : n° 677/2001 JO n° 790 du 12 décembre 2001	Le médiateur des Droits de l'homme B-dul Iancu de Hunedoara nr. 3-5 Sector 1 Bucuresti Romania
République de Saint-Marin	♦ Loi relative à la protection des données personnelles — 1983 (Amendée en 1995)	
Russie	♦ Loi fédérale sur l'information, l'informatisation et la protection des informations — 1995	
Taiwan	♦ Loi sur la protection des données -1995	The ministry of justice 130, Sec 1, Chung Ching South Raad Taipei 100 — Taiwan
Thaïlande	♦ Loi sur la protection des données dans le secteur public — 1998	Authority for the protection of Personal Data Information Commission Government House Bangkok 10300 Thailand

6 — Instruments internationaux

Communauté européenne	Directive européenne n° 95/46/CE relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données — 24 octobre 1995p	Commission européenne DG marché intérieur - Unité A4 200 rue de la Loi — Bruxelles B — 1049 Belgique Site web : http ://europa.eu.int/comm/ internal_market/fr/index.htm
Conseil de l'Europe	Convention n° **108** pour la protection des personnes à l'égard u traitement automatisé des données à caractère personnel — 28 janvier 1981	Conseil de l'Europe Direction des affaires juridiques Section protection des données Avenue de l'Europe 67075 Strasbourg — France Site web : www.legal.coe.int/dataprotection
OCDE	Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel — 23 septembre 1980	OCDE 2, rue André Pascal 75775 Paris cedex 16 Site web : www.oecd.org/index-fr.hlm
ONU	Lignes directives pour la réglementation des fichiers informatisés de données à caractère personnel — 1989	Site web : www.unhchr/french/html/intlinstjr.hlm

Annexe 7

Travaux du groupe « article 29 »

ADMINISTRATION ÉLECTRONIQUE

Administration électronique et protection des données à caractère personnel dans l'Union européenne : l'état des lieux fin 2002

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1] ;

Vu l'article 29 et l'article 30, paragraphe 1, point (a), et paragraphe 3 de ladite directive, et l'article 14, paragraphe 3 de la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 ;

Vu son règlement intérieur, et notamment ses articles 12 et 14 ;

A adopté le présent document de travail :

Introduction

Le développement de l'administration électronique (e-gouvernemenf) constitue aujourd'hui, dans la plupart des États européens, l'un des axes d'action prioritaires des politiques de modernisation administrative. Cette priorité est également manifestée au niveau européen depuis l'adoption par le Conseil européen de Feira (19 au 19 juin 2000) du « plan d'action e-Europe 2002 », qui comporte un volet « administration en ligne ».

Ainsi, l'on assiste à l'heure actuelle au développement de différents types de projets dits « d'administration électronique », qui consistent à mettre en place et à promouvoir la mise en place de téléservices, c'est-à-dire la fourniture en ligne de services administratifs. Or il s'avère que certains de ces projets suscitent des préoccupations majeures du point de vue de la protection des personnes à l'égard du traitement de leurs données personnelles. À titre d'exemple, l'on peut mentionner l'institution d'un point d'entrée unique aux téléservices offerts par l'administration, le développement d'identifiants uniques ou l'interconnexions de bases de données publiques.

Ce document présente un état des lieux des questions relatives à l'administration électronique (e-government) et à la protection des données à caractère personnel dans l'Union européenne. Il a vocation à contribuer à la réflexion générale sur le sujet. Ce document élaboré par la délégation française constitue une synthèse des réponses apportées par les autorités nationales de protection des données réunies au sein du groupe à un questionnaire portant sur ces questions.

Compte tenu de l'évolution constante des services d'administration électronique et des conclusions tirées des expériences menées, le groupe de travail pourra

[1] *Journal officiel* n° L 281 du 23 novembre 1995, p. 31, disponible à l'adresse suivante : http ://europa.eu.int/comm/internal_market/fr/media/dataprot/index.htm

revenir ultérieurement sur ces questions afin de fournir des lignes directrices sur l'application des règles de la directive 95/46/CE dans ce contexte.

AJ Consultation et initiatives des Autorités de protection des données sur les questions d'administration électronique

Toutes les Autorités de protection des données en Europe se sont prononcées sur des questions d'administration électronique.

1) Dans la grande majorité des cas les Autorités ont été officiellement consul tées par es pouvoirs publics. Cette consultation est généralement formellement requise de l'administration dans le cadre de procédures prévues par la loi nationale de protection des données, à l'occasion de la prise de mesures législatives ou régle mentaires par l'administration ayant des implications sur la protection des données, ou à l'occasion de la mise en oeuvre de téléprocédures particulières. À cet égard, il a été soulevé par plusieurs Autorités que cette obligation de consultation de l'Autorité n'est pas systématiquement respectée par les pouvoirs publics. L'administration a également pu consulter l'Autorité de manière spontanée sur des questions d'adminis tration électronique.

2) Les Autorités ont pu également faire connaître leur point de vue à l'occa sion de débats publics ou de réflexions lancés sur le sujet par les pouvoirs publics. Ceci fut notamment le cas en France, où la CNIL a été associée par le gouvernement au débat public conduit sur ces questions et a fait part de ses premières réflexions sur le sujet dans son dernier rapport d'activité, ou au Royaume-Uni, où *l'Information Commissioner* britannique, qui n'a pas été consultée par les pouvoirs publics, a fait part de son avis en commentant différentes propositions gouvernementales ou en par ticipant à des consultations publiques.

3) L'avis de l'Autorité sur les questions d'e-gouvernement peut par ailleurs avoir résulté d'une initiative propre. Aux Pays-Bas, par exemple, l'Autorité a pris l'ini tiative d'exprimer ses avis sur le sujet sans occasion spécifique pour ce faire.

4) Enfin, les Autorités peuvent faire partie de groupes de travail sur des pro jets spécifiques d'e-gouvernement (Finlande, Pays-Bas, France, notamment) ou avoir demandé à être informées de l'évolution de projets spécifiques (Portugal).

Les consultations et initiatives des Autorités ont pu porter sur le cadre général du développement de l'administration électronique, ou sur des sujets partiels.

La lecture des contributions des différentes délégations laisse apparaître que les thèmes des questions étudiées par les Autorités sont très variés. Il peut s'agir tout d'abord d'avis portant sur des projets d'ensemble, tels que, en Espagne, l'établisse- ment d'une carte d'identité électronique ou la mise en œuvre d'un projet global de promotion de l'administration en ligne ; en Suède, la mise en place d'une « politique commune » *(« comrnon policy »)* de l'Association des Banquiers Suédois et de La Poste concernant la carte d'identité électronique ; en Italie, outre l'émission d'une carte d'identité électronique, la mise en place d'un projet national d'établissement d'un « réseau d'administration publique unifié », c'est-à-dire un réseau électronique mettant en relation toutes les autorités administratives du pays.

Il peut également s'agir d'avis sur des téléservices précis, tels que concer nant la fiscalité personnelle, la déclaration de revenus et le paiement des impôts en ligne ; concernant la sécurité sociale, la déclaration et le remboursement en ligne de dépenses maladie (Espagne, France), etc. Dans ces hypothèses les Autorités insistent particulièrement sur les questions de sécurité des données.

Il a pu s'agir également d'avis rendus à l'occasion de l'introduction en droit national de textes particuliers, tels que la directive européenne sur la signature élec-

tronique (Finlande, où la loi de transposition rentrera en vigueur au 1er février 2003 ; Danemark, notamment).

B) État du développement des téléservices publics

Cette question avait pour objet de connaître, dans chaque pays, l'état de développement des téléservices ainsi que le niveau de sécurité existant, et ce sur la base d'une liste des vingt services de base devant être offerts en ligne, tels qu'énumérés par le plan d'action e-Europe établi en vue du Conseil européen de Feira (juin 2000). Toutes les autorités n'ont pas rempli ce tableau, en l'absence d'information suffisante sur certains points.

À l'exception de la Belgique et de l'Allemagne, toutes les autorités de protection des données ont été consultées sur les projets de téléservices mis en œuvre dans leur pays.

De façon générale, les observations formulées lors des avis rendus portent essentiellement sur les sécurités, et en particulier sur les mesures d'identification et d'authentification des internautes ainsi que des agents ou professionnels habilités à accéder aux applications de téléservices. De même, le chiffrement des données lors de la transmission constitue une mesure de sécurité généralement préconisée ainsi que, dans une moindre mesure, le chiffrement lors du stockage des données et l'instauration de dispositifs de journalisation des connexions (Portugal, Pays-Bas, France, Portugal, France, Autriche).

Par ailleurs, les autorités de protection des données s'accordent également pour considérer que le développement des téléservices doit s'accompagner de mesures d'information des administrés, en particulier sur les droits qui leur sont ouverts au titre des législations de protection des données (l'analyse des questionnaires ne permettant pas d'indiquer les mesures prises à cet effet).

1) L'analyse du tableau des téléservices permet de constater que l'ensemble des pays précités offrent aux particuliers un service de déclaration fiscale en ligne, le plus souvent accompagné d'ailleurs du service de paiement en ligne (six pays) et de la téléconsultation de son dossier personnel (six pays également).

De même, parmi les téléservices offerts aux entreprises, le service le plus fréquemment cité concerne la déclaration fiscale en ligne, qu'il s'agisse de la TVA (huit pays) ou de la fiscalité directe (six pays).

Le secteur des finances publiques constitue donc à n'en pas douter le domaine d'intervention privilégié de l'administration électronique. Il est à noter que les téléservices offerts en ce domaine bénéficient généralement d'un niveau de sécurité plus élevé que d'autres téléservices, plusieurs pays indiquant recourir à des dispositifs de signature électronique (Finlande, Espagne, France), ou de chiffrement des données (France, Portugal, Espagne). En Autriche cet accès n'est sécurisé que par mot de passe.

2) La notification administrative de changement d'adresse, dans la mesure où cette démarche constitue une formalité administrative usuelle (voire même obligatoire) dans bon nombre de pays est, après le secteur fiscal, le téléservice le plus fréquemment cité, six pays indiquant disposer d'un tel service[1] qui s'accompagne d'ailleurs dans trois pays (Espagne, Finlande, Norvège) d'une possibilité de consulter son dossier en ligne. Ces services bénéficient d'un niveau de sécurisation variable d'un pays à un autre, cer tains (Espagne, Finlande) mettant en oeuvre un dispositif de signature électronique.

Vient à concurrence le téleservice de recherche d'emplois, également mis en œuvre dans six pays[2], service parfois assorti d'une consultation en ligne de son

[1] Danemark, Espagne, Finlande, Italie, Norvège, Pays-Bas.
[2] Danemark, Finlande, France, Italie, Norvège, Portugal.

dossier (trois pays). Ces services sont généralement accessibles par *login* et mots de passe, donc par des procédures de sécurité classiques.

4) Sont ensuite fréquemment cités (en moyenne à chaque fois au moins par quatre pays) les demandes de permis de construire, les formalités administratives dans les bibliothèques publiques, les demandes de pièces d'état civil, les procédures d'enregistrement de nouvelles sociétés, les contributions sociales, les relations des usagers avec les établissements de soins et les professionnels de santé, les inscriptions dans les établissements d'enseignement, aux examens et concours, les procédures d'immatriculation de voitures, prise en charge de dépenses médicales et enfin les réclamations, dépôts de plaintes (police, justice...), ce dernier service s'accompagnant généralement d'un service de messagerie.

L'analyse des réponses apportées par les autorités de protection des données sur la sécurité des téléservices précédemment énumérés permet de constater une grande disparité de situations, à l'exception de quelques services, sans doute jugés à juste titre plus « sensibles » (ex : immatriculation de voitures, prise en charge de dépenses médicales...), et qui semblent bénéficier de mesures de sécurité spécifiques. Aucune conclusion significative ne peut donc être tirée sauf sans doute à indiquer qu'aucun pays à ce jour — à l'exception peut-être de la Finlande — ne dispose encore d'une vision claire et établie des besoins de sécurité en qui concerne l'administration électronique.

C) Mise en place d'un point d'entrée unique aux téléservices, ou « Portail »

Généralités

L'approche « portail », c'est-à-dire le développement d'un point d'entrée unique aux téléservices administratifs, existe ou est en projet dans quasiment tous les pays concernés par cette étude. Cette tendance générale se manifeste aussi bien dans les pays où l'on avait assisté au développement de sites jouant plus ou moins le rôle de portails indépendants que dans les pays où aucun système ne préexistait.

Dans certains cas, un ministère spécifique est en charge de ce portail. Ainsi, en Finlande, le site http ://www.suomi.fi est maintenu par le ministère des Finances ; en Autriche, le portail du gouvernement fédéral http ://www.help.gov.at est aussi géré par le ministère des Finances.

Ces portails constituent le plus souvent des sites d'information générale : liens vers les différents services publics et institutionnels ; annuaire des adresses des administrations et institutions publiques ; dossiers d'information ; extraits *du Journal officiel* concernant les démarches concernant différentes administrations publiques (formulaires ; information sur les procédures ; information sur l'assistance financière, financements, appels d'offres, offres d'emploi publics, etc.) ; information sur la législation nationale ; actualités ; « boîte à suggestions » ; publications, etc.

De plus en plus fréquemment, ces sites portails sont utilisés pour accéder à des téléprocédures, concernant les citoyens comme les entreprises. Se pose ainsi la question de la possible conservation par le portail de données personnelles. À l'heure actuelle, il n'y aurait aucune conservation de données personnelles par ces sites au Danemark, en Allemagne, en Espagne, au Portugal et en Suède. À l'inverse, de tels sites peuvent ou pourront conserver les données personnelles des citoyens qui y accèdent en Belgique, Italie, Norvège, Finlande, Autriche et Irlande.

Ainsi en Irlande, le système permettra de s'enregistrer en ligne. Il s'agit d'un système d'authentification de l'identité de la personne par le biais de son PPSN *(« Personnel Public Service Number »)* et de la fourniture de services administratifs à travers un intermédiaire, le *« Broker »,* qui conservera les données dans une base de

données centrale sécurisée. L'authentification de l'identité de la personne sera effectuée par le biais d'une base de données spécifique (la « *Public Service Identity Database »),* gérée par le département des affaires sociales et familiales, dans laquelle sont enregistrées des données d'identité de base. Le système exigera des éléments d'authentification supplémentaires pour des transactions nécessitant une plus grande confidentialité ou une plus grande sécurité.

L'accès à ces services par le *Broker* reposera sur le consentement de la personne et les personnes pourront avoir accès aux services sans avoir recours à ce système. Les données personnelles les plus fréquemment utilisées (par exemple informations relatives à la naissance, au passeport, aux revenus, aux relations familiales, etc.) seront maintenues par le *Broker* dans une base de données sécurisée (dite *« data vault* »). Le *Broker* gérera cette information et la protégera pour le compte de l'utilisateur. Seules des données pertinentes seront fournies à une administration demandante obtenir des informations relatives à la personne, sur la base des instructions particulières de celle-ci à l'occasion d'une transaction opérée *via* le *Broker.* Des politiques de sécurité appropriées seront développées pour chaque service et les données enregistrées dans la base seront cryptées.

Quand le système sera développé, il sera possible pour le *Broker* d'anticiper certains événements (par exemple un départ à la retraite), et chaque catégorie du système aura « l'intelligence » de suggérer les points d'intérêt ou pertinents pour la personne. Le *Broker, via* le portail, fournira un point d'entrée unique aux personnes ayant besoin de traiter un dossier avec l'administration. Progressivement il permettra la personnalisation de services particuliers au fur et à mesure qu'un profil pourra être constitué. La position du gouvernement est que la vie privée des personnes sera respectée dans la mesure où les personnes auront donné leur accord à l'utilisation et au stockage de leurs données pour la fourniture de ce service précis. L'autorité de protection irlandaise a approuvé ce modèle, sous de strictes conditions relatives au consentement et à l'utilisation des données pour des finalités spécifiques.

L'autorité néerlandaise a également pris position sur le sujet, en attirant l'attention de l'administration sur l'impact au regard de la protection des données de la distinction opérationnelle entre « *front office »* et « *back office »,* c'est-à-dire les services de contact avec le citoyen d'une part (guichets et bureaux d'accueil), et les services de traitement des dossiers d'autre part. L'administration de *« front office »* collecte toutes sortes de données nécessaires à la fourniture des services requises par le citoyen, que l'administration de « *back office* » va ensuite utiliser afin d'apprécier la position du citoyen au regard de chacun de ces services ; ainsi, l'administration peut fournir un seul guichet aux fins de fournir plusieurs services. L'administration tend à avoir de plus en plus recours à cette structure organisationnelle, dont les services de portail et de « guichet unique » sont emblématiques. Dans son rapport annuel, l'autorité néerlandaise a insisté sur le fait qu'il convient, dans ces circonstances, de définir les responsabilités respectives de chaque administration concernée au regard des données traitées, afin de prévenir toute utilisation et circulation inutile des données du citoyen au sein des services de *« back office ».*

Recours à des prestataires privés pouvant avoir accès à des données à caractère personnel des usagers

La proximité entre l'administration électronique et les services marchands en ligne et, par conséquent, la possibilité que des services administratifs en ligne soient fournis par des entreprises privées, imposent de rappeler différentes considérations au regard de l'organisation de l'administration électronique. Ainsi, des entreprises privées peuvent-elles assurer l'égalité de tous devant le service public ? Comment se rémunére-

raient-elles ? Leur intervention implique-t-il que certaines téléprocédures soient payantes, etc. ?

Ces questions n'ont pas obtenu les mêmes réponses dans les différents pays de l'Union.

Ainsi, le choix de ne pas avoir recours à des prestataires privés pouvant avoir accès à des données à caractère personnel des usagers a été retenu en Allemagne, en Italie, en Espagne, aux Pays-Bas, en Suède et en Norvège.

Le choix contraire a été fait en Belgique, au Danemark, en France (de manière occasionnelle seulement), en Finlande et en Autriche, où n'importe quel prestataire privé compétent peut postuler pour fournir de tels services après avoir prouvé qu'il mettra en place les garanties nécessaires de sécurité, en particulier au regard de la protection des données. Aucune certitude n'existe sur ce point au Portugal et au Royaume-Uni, où il n'existerait cependant aucune objection de principe au ait d'avoir recours à des prestataires privés dans ce cadre.

Le service Passport offert par Microsoft n'aurait été mis en œuvre dans aucun pays dans le cadre de projets d'administration électronique, certaines Autorités ne disposant par ailleurs d'aucune information spécifique cet égard.

Avis de l'Autorité sur ces sujets et réaction de l'administration

Les Autorités de protection des données ne se sont pas toujours exprimées sur les questions relatives à l'institution d'un portail, notamment parce qu'il n'est pas toujours prévu que ceux-ci conservent des données personnelles.

À l'inverse, dans les pays où le portail implique un traitement et une conservation de données personnelles, les Autorités se sont généralement exprimées pour insister sur le fait que le recours à des prestataires privés ne pouvait avoir lieu qu'une fois des garanties spécifiques mises en place. Ainsi, les exigences croisées de plusieurs autorités font apparaître les garanties suivantes : contrat de sous-traitance approprié ; détermination précise de la mission des prestataires privés ; détermination de conditions de sécurité (environnement sécurisé et entièrement automatisé) ; encadrement juridique de ces prestataires (agrément) comportant notamment une interdiction d'utiliser les données confiées à d'autres fins ou de les divulguer ; définition précise des données enregistrées ; constitution éventuelle d'un comité de surveillance, etc.

D) Systèmes d'identification nationaux des personnes physiques (recours à des identifiants uniques ou sectoriels pour accéder à certains téléservices publics)

Au préalable, il convient de rappeler que jusqu'à présent, ne disposent d'un identifiant unique et général au niveau national que la Belgique, le Danemark, l'Espagne, la Finlande, l'Irlande, l'Italie, le Luxembourg, la Norvège et la Suède. Des projets de développement d'un tel identifiant existent dans d'autres pays, notamment en Autriche, mais seulement dans la mesure où celui-ci serait utilisé de manière cachée pour mettre en place des identifiants sectoriels dérivés (voir plus bas). Au Danemark, en Belgique et en Espagne, cet identifiant unique co-existe avec des identifiants sectoriels. Dans les autres pays, seuls des identifiants sectoriels existent : Allemagne (sécurité sociale, numéro de passeport), France (sécurité sociale essentiellement), Grèce, Portugal (notamment numéro judiciaire), Pays-Bas (identifiant social-fiscal, notamment). Dans des pays comme l'Allemagne et le Portugal, il convient de rappeler que le recours à un identifiant unique est considéré comme anticonstitutionnel.

Le développement de l'administration électronique constitue parfois l'occasion de refondre ce système d'identifiant ou d'étendre la portée d'un identifiant sectoriel. À l'heure actuelle, seuls le Portugal et l'Autriche ont indiqué que ces développements occasionnaient une refonte de leur système national d'identification des personnes.

1) La tendance générale est, pour la finalité d'accès aux téléservices, d'avoir recours à des identifiants pré-existants, uniques (Belgique, Danemark, Espagne, Irlande) ou sectoriels (France, Pays-Bas, Portugal, Italie).

2) Dans certains pays où l'identifiant unique n'existe pas, il a été soutenu que la mise en place d'un portail personnalisé de l'administration ne devait pas constituer l'occasion d'instaurer un tel identifiant (France, notamment). L'Autriche constitue un cas particulier à cet égard, car les pouvoirs publics sont sur le point d'y instituer un identifiant unique (le numéro du registre des résidents), qui ne peut toutefois être stocké ailleurs que dans la base du registre des résidents lui-même et ne peut être utilisé que pour effectuer une dérivation d'identifiants sectoriels, en application d'une procédure très protégée. Aucune administration n'est autorisée à stocker les identifiants d'un secteur autre que celui de son secteur de compétence.

3) Des projets d'extension d'identifiants sectoriels pour l'accès à des téléservices ont été, ou sont envisagés dans certains pays. Un projet de généralisation de l'identifiant social-fiscal aux Pays-Bas a été abandonné par le gouvernement, suite à l'opinion défavorable de l'Autorité sur ce point. À l'heure actuelle, un tel projet n'existe qu'en Italie, où il est prévu que l'identifiant fiscal soit généralisé pour constituer un identifiant unique d'accès à certains téléservices.

4) Un débat a incidemment eu lieu en Italie sur le risque de généralisation *de facto* d'un identifiant sectoriel (en l'occurrence fiscal) une fois celui-ci intégré à une carte d'identité électronique : l'Autorité italienne a rappelé au gouvernement qu'en vertu de l'article 8 (7) de la directive 95/46 relatif à l'institution d'un identifiant unique, il convenait de déterminer les conditions dans lesquels un tel numéro ferait l'objet d'un traitement. Le gouvernement italien a assuré le Garante vouloir tenir compte de cette opinion, mais à l'heure actuelle la situation n'est pas définitivement fixée.

5) La libéralisation de l'usage de l'identifiant unique est effective dans certains pays, notamment en Irlande, où le PPSN *(« Personal Public Service Number »)* est un identifiant unique institué par la loi utilisé pour la finalité d'accès aux services publics, et qui peut ainsi être utilisé pour les finalités fiscale et sociale ainsi que pour les besoins de certains services publics nationaux et locaux. Cette libéralisation est également prévue en Belgique, où l'utilisation du numéro de registre national (et pour les personnes physiques ne disposant pas d'un numéro de registre national, du numéro d'identification de la sécurité sociale) comme identifiant unique pour les personnes physiques est désormais obligatoire dans tous les systèmes d'information des pouvoirs publics. L'Autorité de protection doit rendre un avis sur cette question de manière imminente.

6) Le recours à des identifiants sectoriels uniquement est retenu en Allemagne, au Portugal, au Royaume-Uni et en France. Les identifiants sectoriels ne seront alors utilisés que pour leur finalité originale.

7) Dans la même logique d'évitement de risques d'interconnexions, d'autres Autorités ont soutenu ou suggéré qu'il soit fait recours à des identifiants sectoriels dérivés d'un identifiant unique. Ceci fut notamment les cas aux Pays-Bas, où le projet initial du gouvernement a été ainsi infléchi, et en Autriche, où l'identifiant unique (secret), combiné avec une fonction spéciale de signature électronique *(via* la « carte

citoyenne » autrichienne, la *« Bürgerkarte »),* sera utilisé pour avoir un accès sécurisé à toutes les applications d'administration électronique ainsi que pour certaines applications en ligne fournies par le secteur privé.

8) Particularités :

— en Finlande, un projet de révision des systèmes d'identification des personnes re latifs à l'administration électronique est en cours, qui prévoit d'avoir uniquement re cours à un identifiant unique spécialement créé pour la finalité de signature électronique et d'identification électronique auprès du registre national de la popula tion. Il n'est pas prévu que cet identifiant soit utilisé pour avoir accès à des procédu res administratives en ligne. L'identifiant unique pré-existant, le numéro de sécurité sociale, ne doit pas être utilisé pour ces finalités ;

— en Belgique, le développement de l'administration électronique a été l'occasion de créer un identifiant unique pour les entreprises : Le numéro de TVA actuel (étendu aux entreprises et organisations non assujetties à la TVA) est converti en un numéro d'identification unique pour toutes les entreprises et les organisations ; ce numéro remplacera tous les autres numéros spécifiques et sera introduit comme identifiant unique des entreprises et organisations dans tous les systèmes d'information des pou voirs publics.

E) Interconnexions induites par le développement de l'administration électronique

Une préoccupation notable, exprimée de manière imagée par l'Autorité britannique, est que le développement de l'administration électronique ne devrait pas opérer comme un écran de fumée qui cacherait une interconnexion généralisée des bases de données publiques et un échange accru de données personnelles entre administrations. La CNIL a également rappelé sa doctrine générale, qui consiste à refuser toute interconnexion généralisée des fichiers. La CNIL a rappelé cette doctrine générale à l'occasion de consultations organisées par les auteurs d'un rapport, rédigé à la demande du gouvernement, sur *Administration électronique et protection des données personnelles.* Suite à la remise au gouvernement de ce rapport, un débat public a été organisé sur les principaux points identifiés lors de sa rédaction. L'une des principales conclusions de ce débat public, rejoignant parfaitement la doctrine de la CNIL, a été que l'administration électronique ne doit pas se traduire par une augmentation du niveau de contrôle sur les individus, ce contrôle résultant au premier chef d'interconnexions.

En Allemagne, par ailleurs, il est important de souligner que c'est au sujet des interconnexions que la Cour suprême allemande a retenu sa célèbre théorie au « droit à l'autodétermination informationnelle » des individus. Ce droit consiste, pour chaque individu, à pouvoir décider de la communication et de l'utilisation de ses données par des tiers. L'affirmation de ce droit, si elle n'équivaut pas à une interdiction absolue des interconnexions, limite du moins beaucoup les possibilités d'interconnexions.

À cet égard, quand des interconnexions ont été signalées comme susceptibles de se produire, la motivation essentielle de ce développement résulte d'une volonté de simplification de procédures. Cette motivation concerne tant les entreprises que les particuliers, notamment, pour ces derniers, à l'occasion d'un changement d'adresse. L'objectif de combattre la fraude a également été mentionné (notamment en Irlande et au Royaume-Uni)

À l'heure actuelle, ces interconnexions ne sont généralement pas définies, ou sont en cours de définition seulement. Les domaines concernés varient selon les préoccupations nationales : le domaine de la santé (Espagne, Finlande), celui de la

gestion des relations entre administration et entreprises (Belgique), l'indexation de fichiers publics (Italie), notamment.

Certaines Autorités de protection des données participent à des groupes de travail où ces questions sont examinées (par exemple aux Pays-Bas ou en Finlande) ; d'autres, comme la CNIL, bénéficient de l'examen des traitements de données personnelles préalablement à leur création.

Les questions relatives à ces projets mentionnées par les délégations concernées sont systématiquement les mêmes :
— au plan juridique, les interconnexions sont traitées, soit dans le cadre d'une autorisation par la loi (France), soit dans le cadre de dispositions requérant le consentement des personnes. Ainsi, en Espagne, le projet de réglementation sur la promotion de l'administration électronique satisfait aux exigences de la loi générale de protection des données, en exigeant le consentement des personnes concernées préalablement à la transmission des données par voie télématique entre administrations ;
— quant aux principes de la protection, il a été particulièrement insisté sur les principes de qualité des données, de légitimité du traitement, de l'information des personnes, ainsi que sur le niveau de sécurité mis en oeuvre.

Les questions relatives à la nécessité et aux conditions générales de mise en œuvre d'interconnexions ont été particulièrement étudiées au Royaume-Uni à l'occasion de la publication, en 2002, d'un rapport commandé par le gouvernement britannique de la *« Performance and Innovation Unit »* (un organisme de réflexion stratégique au cœur du gouvernement britannique, désormais dénommé la « *Strategy Unit »).* Ce rapport intitulé *Privacy and data sharing : the way forward for public services,* présente les questions d'interconnexion comme mises en avant par le développement de l'administration électronique et des attentes des citoyens à cet égard, mais insiste sur l'importance équivalente des attentes de ceux-ci quant à la protection de leur vie privée. Il convient donc d'établir un équilibre entre interconnexions (et donc amélioration supposée des services de l'administration) et protection des données des usagers. La recherche de cet équilibre imposerait de passer par les phases d'analyse suivantes :
— Quels sont les avantages de l'utilisation envisagée des données et de leur interconnexion au regard des objectifs de l'administration ?
— Existe-t-il des approches alternatives pour atteindre les mêmes objectifs ?
— Quels sont les risques et les coûts induits par une interconnexion ?
— Quelles pourraient être les garanties nécessaires pour encadrer ces risques (ex. : PETs) ?
— À l'issue de cette analyse, existe-t-il un équilibre entre les bénéfices et les risques induits de l'interconnexion envisagée ?

Enfin, un des intérêts essentiels de ce rapport est de rappeler que les interconnexions ne sont pas inévitables pour améliorer les services de l'administration.

F) Signature électronique et infrastructures à clés publiques

La majorité des délégations indique que la participation d'intervenants de droit privé, « prestataires de services de certification » est, ou serait permise dans le cadre de la mise en œuvre de mécanismes de signature électronique pour certains téléservices publics, dans les pays concernés. Dans ces cas, le statut de prestataire de services de certification est encadré juridiquement (par exemple, condition d'agrément). Ces questions ont fréquemment été réglées à l'occasion de la transposition en droit national de la directive relative à la signature électronique.

Dans les autres cas, le recours a des prestataires privés est impossible, du fait que seul l'État assure ce rôle (Allemagne, Espagne). En France, ce rôle opère par défaut : à ce jour des prestataires privés n'opèrent que pour la certification de télédéclarations de TVA. Dans les autres cas de figure, l'État joue le rôle d'autorité de certification.

En règle générale il est souligné que le recours à des mécanismes de signature électronique est peu développé à l'heure actuelle, soit en raison d'un défaut de cadre réglementaire, soit en raison d'un coût et d'une complexité encore trop élevés. Ainsi la CNIL souligne, à cet égard, que le recours systématique à de tels procédés ne peut pas constituer une condition préalable à la mise en place des téléprocédures ; en l'état du droit, de la technique et de l'économie des infrastructures à clé publique, il serait prématuré d'imposer de telles solutions. À l'inverse, il est relevé que certaines procédures administratives ne sont pas encore en ligne car elles nécessiteraient la mise en place de moyens de signature et de cryptage. Ainsi, à certaines exceptions près, de nombreuses administrations ne disposent d'aucune procédure grand public associant un mécanisme de signature électronique.

Les domaines de ces applications manifestent des priorités variables selon les pays : secteurs fiscal et social (France), registre de la population (Finlande), par exemple. Dans la majorité des cas, ces mécanismes concernent de manière équivalente les particuliers, les entreprises et les agents de l'administration. Parfois les particuliers sont les premiers concernés (Allemagne), parfois ce sont les employés, les organisations et les serveurs, et donc pas majoritairement les personnes physiques (Danemark), parfois ce sont les agents de l'administration (Norvège). Une distinction a été rappelée sur ce dernier point : les signatures électroniques concernant des agents publics n'ont pas tant besoin d'identifier l'individu derrière la signature que d'identifier si la personne derrière la signature a le pouvoir nécessaire pour prendre la décision ou réaliser l'action en cause.

Les Autorités de protection des données ont pu faire connaître leurs positions à différentes occasions. Parfois elles ont été consultées par le gouvernement à l'occasion de l'adoption de règles législatives ou réglementaires sur l'encadrement d'activités faisant appel à des mécanismes de signature électronique ; parfois elles se sont prononcées suite à la soumission d'applications particulières à leur examen préalable.

L'attitude générale des Autorités de protection des données envers les mécanismes de signature électronique est positive, car celles-ci sont interprétées comme des mécanismes propres à favoriser la protection des données personnelles. De même, l'autorité autrichienne considère que l'identification unique des personnes demandant à avoir accès en ligne à leurs données constitue une contribution importante à la protection des données dans le contexte de l'administration électronique. Toutefois, l'importance d'intégrer les questions de protection des données dans le développement de ces mécanismes a été soulignée par plusieurs autorités. Il a été notamment préconisé qu'une formulation claire doit être fournie à l'utilisateur sur la communication de données par les fournisseurs de services de certification, en application des dispositions légales sur la communication des données personnelles.

G) Cartes d'identité électroniques

1) À l'heure actuelle, les cartes à vocation sectorielle constituent la majorité des cartes d'identité électroniques détenues par les personnes dans les pays européens. Il s'agit notamment de cartes de sécurité sociale, à laquelle il est occasionnellement envisagé d'associer à terme un volet santé (par exemple en Autriche). Ces

cartes sectorielles co-existent parfois avec des cartes à vocation générale, notamment en Belgique et en Finlande.

2) À terme, il devrait y avoir autant de pays disposant de cartes à vocation générale que de pays disposant de cartes à vocation sectorielle seulement. En effet, si des cartes d'identité électronique à vocation générale n'ont été délivrées à l'heure actuelle qu'en Belgique, Italie et Finlande, cette délivrance est projetée en Alle magne, aux Pays-Bas, en Suède, en France et au Royaume-Uni (où, en raison de la difficulté politique d'évoquer l'instauration de cartes d'identité dans ce pays, l'on parle plutôt *« d'entitlement card »* : la carte ne serait pas utilisée pour les contrôles d'identité mais pour identifier des personnes qui voudraient avoir accès à certaines prestations et aurait également valeur de carte de sécurité sociale). Au Portugal, une carte unique est également en projet. Il s'agirait d'enregistrer différents types de don nées sur la carte, correspondant à différents identifiants, une administration ne pou vant avoir accès qu'aux données qui la concernent. Des travaux sur la faisabilité technique de cette carte sont en cours. L'Autorité de protection a demandé d'être informée sur les progrès de ces travaux, afin de veiller au respect des dispositions constitutionnelles interdisant l'institution d'un identifiant unique au Portugal.

3) Les expériences les plus abouties à l'heure actuelle en matière de cartes d'identité électronique concernent l'Italie et la Finlande.

• En Finlande, la carte d'identification électronique consiste en une carte d'identité comportant la photo de son titulaire et une puce sur laquelle sont enregistrés le certificat d'authentification du titulaire, le certificat de non-répudiation nécessaire pour les applications de signature électronique, et le certificat du Centre d'enregistrement de la population *(Population Register Center),* qui aura délivré le « e-number » de la personne. Ce numéro unique, développé par le *Population Register Center,* est essentiellement utilisé dans le cadre de transactions commerciales. La carte ne contient en revanche pas l'identifiant universel de la personne (attribué à la naissance), ni son adresse ni sa date de naissance. Elle est sécurisée par un numéro personnel d'identification (PIN), que l'utilisateur peut également utiliser pour avoir accès aux réseaux d'information tels internet.

En plus d'être une carte d'identité (au même titre qu'un passeport ou un permis de conduire), cette carte sert donc également pour les finalités d'identification électronique et de signature électronique. Elle est utilisable dans le contexte de transactions commerciales, mais aussi vis-à-vis de l'administration. Ainsi, par exemple, la carte peut être utilisée pour faire valider un changement d'adresse en ligne en utilisant l'application *créée* à cet effet par le *Population Register Centre* et la Poste finlandaise. En novembre 2002, le gouvernement a de surcroît proposé que cette carte d'identité soit fusionnée avec la carte de Sécurité sociale. À la demande du *Data Protection Ombudsman,* il a été mentionné dans le projet que la personne restait libre de décider si des données de sécurité sociale et des données de santé devaient être intégrées à la carte.

À l'heure actuelle, la carte coûte 29 € et est valable trois ans ; il est question que son coût soit relevé à 40 € et que sa durée de validité soit prolongée jusqu'à cinq ans. Elle n'est pas délivrée qu'aux citoyens finlandais : les personnes étrangères résidant en Finlande de manière permanente et dont l'identité a pu être valablement établie peuvent également être titulaires de la carte.

Ces cartes sont délivrées par les branches locales de la police sur présentation d'une carte d'identité, d'un passeport ou d'un permis de conduire. Le *Population Register Centre,* qui sert de prestataire de services de certification à l'administration finlandaise, fournit les certificats nécessaires à l'identification électronique. En plus

de la carte, un lecteur est nécessaire, que les utilisateurs doivent détenir à leur domicile. À terme, toutefois, l'identification serait possible à partir d'un appareil mobile, tel un téléphone portable, équipé d'une puce spéciale. Un système de déclaration de perte ou de vol est disponible 24h/24h.

La carte d'identité finlandaise n'a pas rencontré le succès escompté. À l'heure actuelle, seuls 13 000 Finnois l'ont adoptée. Au titre des facteurs expliquant ce manque de popularité, sont évoqués une perception relativement floue des bénéfices induits par la détention de la carte, et le fait que la carte soit payante, ainsi que les lecteurs que les utilisateurs doivent détenir à domicile pour l'utiliser sur internet pour des finalités commerciales. Ainsi, l'établissement de la carte étant facultative, les Finlandais ont généralement préféré s'en tenir aux moyens d'identité classiques.

• La carte d'identité électronique italienne, au contraire de la carte d'identité finlandaise, a vocation à se substituer à la carte d'identité papier et serait ainsi obligatoire pour chaque citoyen.

D'après le projet en cours, outre le fait d'être une carte d'identité au sens strict, ainsi qu'un titre de nationalité et un titre autorisant le libre déplacement au sein de l'Union européenne, la carte d'identité italienne permettrait également l'accès aux services publics nationaux et locaux, offrirait une fonction de signature électronique, et permettrait aux citoyens de voter en ligne. D'autres fonctions pourraient être offertes, telle la possibilité de prendre rendez-vous en ligne avec un médecin, par exemple.

Cette carte, qui peut être délivrée à des mineurs, contient des données d'identité mais également l'identifiant fiscal de la personne. Elle contiendra à terme les empreintes digitales et toutes les données de santé, à l'exception de l'ADN, que son titulaire autorisera à y enregistrer (cette condition de l'autorisation de la personne ayant été mise en œuvre suite à l'intervention de l'autorité italienne de protection des données). Le gouvernement a l'intention de promouvoir l'utilisation de la carte sur internet en installant des terminaux à l'intention du public dans les bars, restaurants et boutiques, la carte d'identité électronique ayant alors une fonction d'identification en ligne. Un autre objectif de cette action est que les commerçants tiennent lieu de guichets administratifs, ce qui permettrait à terme de réduire les coûts de ces opérations pour l'administration.

Au titre des préoccupations du ministère de l'intérieur italien dans la mise en œuvre de ce projet, l'on trouve essentiellement, entre autres, la préoccupation de centraliser de manière logique les autorisations lors de la délivrance des cartes, de garantir l'indépendance dès collectivités locales dans la mise en œuvre de leurs services en ligne aux citoyens et de mettre en œuvre une politique de sécurité sur la carte elle-même et tout au long de son cycle de vie. Cette politique de sécurité a consisté par exemple à définir un processus complexe de production, d'initialisation, d'activation et d'émission de la carte, celle-ci se faisant par les autorités locales qui ont les moyens de recueillir les données personnelles et de les mettre sur la carte, y compris la photo.

La carte utilise deux technologies sur un support plastique classique : un micro processeur de 16 K et une bande laser. La carte plastique supporterait une photo, les nom, prénom, sexe, date et lieu de naissance de la personne ainsi qu'un numéro d'identification unique. Sur l'autre face se trouve l'adresse et le numéro de code fiscal de la personne, la période de validité de la carte ainsi que les deux composants (le microprocesseur et la bande laser). L'on retrouverait en hologramme sur la bande laser les informations sur la personne ainsi que son empreinte digitale et sa signature.

Les deux technologies ont chacune leur raison d'être. La bande laser sert de carte d'identité et le microprocesseur de carte de services.

Le microprocesseur permettrait d'assurer une identification et une authentification sur la base de clés symétriques et asymétriques. Il serait possible de stocker jusqu'à seize clés sur une carte.

4) Lorsque des projets de cartes à vocation générale existent, leurs finalités se recoupent généralement :
— il s'agit évidemment au premier chef de l'attestation de l'identité de la personne ;
— il est également prévu de manière quasi systématique que cette carte serve à accéder aux téléservices publics (sauf en Allemagne, en l'état des informations disponibles), à s'identifier et à s'authentifier dans le cadre de transactions de commerce électronique (ce point n'étant pas encore défini en Espagne) ;
— la fonction de signature électronique est systématiquement prévue, tant pour les téléservices publics que pour les applications de commerce électronique (ce dernier point étant toutefois indéfini en Espagne) ;
— par contre, ces cartes générales n'ont fonction de cartes de paiement qu'en Allemagne, en Italie, au Portugal et en Suède ;
— Ta fonction « carte de santé » n'est définitivement retenue qu'en Allemagne et en Finlande, et est envisagée au Portugal et en Italie ;
— La fonction « sécurité sociale » n'est retenue qu'en Allemagne et en Finlande. Dans les autres pays, il est fréquent qu'une carte sectorielle joue ce rôle ;
— enfin, ces cartes serviraient également de cartes d'électeur en Allemagne, en Italie, aux Pays-Bas, et potentiellement au Portugal et en Suède.

5) La majorité des Autorités de protection européennes ont été consultées sur ces questions. Certaines ont approuvé les projets des autorités publiques (Finlande, Suède), d'autres sont en cours de discussion sur des projets existants, d'autres ont fait valoir une opinion différente de celle de l'administration en charge du projet (Italie, Pays-Bas). En tout état de cause, plusieurs éléments ont été relevés comme potentiellement problématiques :
— détermination de la nature des données enregistrées sur la carte ;
— détermination des procédures de traitement de ces informations ;
— détermination des organismes autorisés à avoir accès aux différentes catégories d'informations ;
— respect des droits des personnes ;
— détermination des administrations habilitées à décider des données enregistrées dans la carte d'identité électronique ;
— possibilité d'utilisation de la carte d'identité électronique à des fins commerciales (paiement en ligne, portefeuille électronique, etc.) ;
— mesures de sécurité mises en œuvre (l'Italie soulignant à cet égard qu'une seule entreprise au monde serait aujourd'hui en mesure d'offrir des réponses à la mesure des ambitions technologiques du projet en cours) ;
— stockage central de données de santé et de données biométriques (empreintes digitales).

H. La maîtrise par les administrés de leurs données personnelles

Ce point n'est pas résolu de manière identique dans les différents pays européens. De fait, comme l'indique l'Autorité britannique, il peut y avoir des tensions au sein de l'administration entre le désir de fournir des services cohérents et pratiques pour l'utilisateur, et la tendance à vouloir fusionner des sources d'informations sur les personnes, d'une manière susceptible de constituer une infraction à la législation de protection des données personnelles. La maîtrise de leurs données personnelles par les citoyens est ainsi au cœur de cette tension. À la lecture des réponses des Autorités, il existe deux grandes tendances sur ces questions :

Une première tendance, à laquelle souscrivent expressément plusieurs pays, généralement avec l'accord des Autorités de protection des données (Irlande, Danemark, Espagne, Finlande), consiste à considérer que l'administré doit rester maître de ses données à tous les stades des procédures administratives, et qu'il doit avoir un retour d'information sur les échanges de données ayant sous-tendu toute décision prise à son égard. Une conséquence de cette tendance est que l'échange de données entre administrations par voie télématique peut être soumise au consentement des personnes concernées (ex. : Espagne, Irlande). Dans d'autres pays la situation est plus hésitante (Royaume-Uni, Belgique). À l'appui de cette tendance, il peut être relevé qu'un tel contrôle personnel conditionne la confiance que doit générer l'administration électronique, ainsi que sa crédibilité. De même, par effet d'entraînement, plus les citoyens ont confiance en leur administration, moins ils éprouveraient le besoin d'exercer un tel contrôle.

Cependant, quand bien même l'utilisateur retiendrait ce contrôle sur ces données, les principes fondamentaux de protection des données doivent être appliqués. Ainsi, afin de satisfaire à la condition de collecte loyale des données, la préconisation de l'Autorité irlandaise consiste à ne pas constituer la base à partir de données déjà détenues par l'administration pour une finalité différente. Par contre, il a été recommandé et accepté par le gouvernement que la possibilité soit offerte aux citoyens de consentir à l'enregistrement de leurs données dans le nouveau système et d'être informés des finalités et des utilisations qui seront faites de la base. Le principe de qualité des données doit également être respecté : ainsi, des données excessives ou non pertinentes, qui seraient peu susceptibles de correspondre à une utilisation légitime dans le cadre d'un service public, ne devrait être ni demandées ni a fortiori stockées. La personne devrait être libre de déterminer quelles données supplémentaires elle désirerait fournir afin d'avoir accès à une gamme de services plus large. De même, les personnes doivent être conscientes de la gamme des utilisations potentielles de leurs données au moment de la collecte, et les agents des administrations et autorités publiques devraient être clairement informés des formes d'utilisation légitime des données auxquelles ils ont accès. Cette information doit ainsi être suffisamment précise pour que les personnes puissent réellement comprendre les conséquences et les risques potentiels induits par la transmission de leurs données. À défaut d'une telle information, le consentement de la personne serait une illusion, car elle n'aurait évidemment aucune raison de refuser la communication de ses données face à l'argument de simplification des démarches administratives.

Certaines Autorités soulignent de surcroît qu'un autre point clé consiste à assurer un niveau de sécurité satisfaisant des applications concernées. Ce point n'est pas théorique, comme le montre une opinion de l'Autorité espagnole dans une affaire récente. Une autorité locale espagnole avait sous-traité à deux organismes financiers la mise en place d'une procédure de demande de certificats de résidence, utilisés par les demandeurs pour obtenir des réductions sur leurs titres de transport. Ces sous-traitants délivraient ces certificats au moyen de distributeurs de billets. Or, lors du traitement de la demande, le distributeur permettait de visualiser non seulement ses propres données personnelles, mais aussi celles des personnes enregistrées dans la base qui habitaient la même résidence. L'Autorité espagnole a sanctionné l'autorité locale pour communication illégale des données.

À l'inverse, une deuxième tendance consiste à considérer que la simplification administrative se fait nécessairement, pour l'utilisateur, au prix d'une certaine perte de la maîtrise sur ses données personnelles. L'on ne pourrait ainsi satisfaire à la fois aux exigences d'une administration électronique plus rapide et aux exigences d'une information « à l'ancienne » de l'administré. Trois pays (Portugal, Allemagne

et Italie) considèrent que le contrôle du citoyen sur ces données n'est pas une conséquence nécessaire du développement de l'administration électronique. Un argument relevé par l'Autorité française, à cet égard, est le risque que ce contrôle ne soit souvent qu'un leurre en pratique. En effet, l'usager aurait à tort le sentiment qu'il maîtrise ses données, alors que l'administration constitue à l'évidence un champ d'intervention où il peut être contraint, par la loi et les règlements, à fournir des données. Ainsi, l'Autorité portugaise considère qu'il est plus facile de favoriser le droit d'accès des personnes à leurs données accessibles en ligne (ce qui ne représente pas toutes les informations sur les personnes) que de soumettre la communication de leurs données au consentement des personnes, si bien que l'utilisateur n'exercerait aucun contrôle sur la communication de ses données à un tiers au sein de l'administration.

/. Institution d'une autorité de protection des données spécifique aux projets d'administration électronique

Hormis la Belgique et, dans une certaine mesure, la Finlande et le Danemark, la question ne s'est aucunement posée de savoir s'il devait exister une Autorité spécifique de protection des données pour les questions d'administration électronique. Les Autorités de contrôle pré-existantes semblent avoir été naturellement désignées comme les Autorités compétentes pour se prononcer sur les projets d'administration électronique ayant des incidences sur la protection des données.

D'autres autorités que les Autorités de protection des données peuvent être amenées à exercer leur compétence dans le domaine de l'administration électronique, qui peuvent éventuellement toucher à des questions de protection des données. Ainsi, par exemple, au Royaume-Uni, le médiateur de l'administration peut, entre autres, enquêter sur des plaintes de particuliers concernant les activités de l'administration, y compris des activités d'administration électronique. De même, en Finlande, les autorités de régulation des télécommunications restent chargées du contrôle de la conformité des questions concernant les autorités de certification et les télécommunications en général, de même que les questions d'archivage électronique relèvent du domaine des administrations compétentes. Parfois, comme au Danemark, l'Autorité de protection des données a expressément accepté des compétences additionnelles à la demande des autorités publiques, en l'occurrence celle d'autoriser des solutions de sécurité dans le domaine de l'administration électronique. Dans tous ces cas, il n'est pas question de partager une compétence de contrôle de la conformité de ces activités avec la législation de protection des données à caractère personnel.

Par contre, ce partage de compétence a été envisagé en Belgique. Un projet est actuellement en cours, consistant à instituer une commission de contrôle, autre que l'Autorité de protection des données, qui consisterait en des comités d'autorisations d'accès aux données non-publiques détenues par l'administration dans la base dite « banque-carrefour des entreprises ». À l'origine, ces comités d'autorisations devaient être distincts de la Commission. Celle-ci, dans sa décision relative à l'institution de la base, a plaidé pour que ces comités soient institués auprès d'elle. Elle a spécifiquement souligné que la création de commissions distinctes nuit à la nécessaire unité d'approche qui devrait caractériser, notamment sur le plan institutionnel, le contrôle du respect de la vie privée. Elle a ainsi rappelé qu'il lui semblait indispensable que soit bien pesée l'incidence de ce choix au moment où le Gouvernement entend développer une politique d'« e-gouvernement », avec les applications que celle-ci pourront avoir demain dans d'autres secteurs de l'administration, comme par exemple la carte d'identité électronique. Face à cette multiplication, prévisible, de dossiers, la Commission a estimé important que les questions liées aux droits et libertés fondamentaux des citoyens suscitées par ces nouveaux dossiers puissent être étu-

diées, autant que faire se peut, dans une enceinte unique. Dans le projet actuel, ces comités seraient désormais institués auprès de la Commission. Il s'agirait de comités composés d'un certain nombre de membres de la Commission, auxquels s'ajouteraient des représentants et/ou experts du secteur concerné.

SÉCURITÉ ET TRANSPORTS AÉRIENS

Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis

Adopté le 24 octobre 2002

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel ;

Institué par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995[1] ;

Vu les articles 29 et 30, paragraphe 1, point a et paragraphe 3 de la directive ;

Vu son règlement et notamment les articles 12 et 14 ;

Adopte le présent avis :

Problématique

Contexte et objet

Dans la foulée des événements du 11 septembre 2001[2], les États-Unis ont adopté le 19 novembre 2001, l'*Aviation and Transportation Security Act*[3] imposant aux compagnies aériennes opérant des vols à destination de leur territoire, de leur transférer des données relatives aux passagers et aux membres d'équipage fPassenger Manifesf *Information)*[4]. Le transfert doit être effectué par voie électronique et terminé avant le décollage de l'avion, au plus tard dans les quinze minutes après le départ, pour les passagers. Bien que le destinataire des données transmises aux États-Unis soit le « *Commissioner of Customs »,* les données seront partagées entre les autorités fédérales américaines. Le but de la transmission n'est pas limité à la sécurité aérienne mais concerne l'ordre public américain.

Le 14 mai 2002, les États-Unis ont adopté une autre loi visant à améliorer la sécurité aux frontières qui impose aux compagnies aériennes arrivant aux États-Unis ou quittant ce pays de transmettre des données relatives aux passagers et aux membres d'équipage au service de l'immigration des États-Unis *(US Immigration and Naturalization Service)*[5]. En ce qui concerne les passagers et les membres d'équipage arrivant aux États-Unis, les données et l'obligation de transmission est la même

[1] *Journal officiel* L 281 du 23 novembre 1995, p. 31, peut être consulté à l'adresse suivante : http ://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] Avant le 11 septembre, les compagnies aériennes transféraient déjà certaines données vers les Etats-Unis sur une base volontaire.

[3] *Aviation and Transportation Security Act* du 19 novembre 2001 (107-71), *Intérim Rules of Dep. Of The Treasury (Customs) — Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States* (registre fédéral, 31 décembre 2001) et *Passenger Name Record Information Required for Passenqers on Flights in Foreign Air Transportation to or From the United States* (reqistre fédéral, 25 juin 2002).

[4] Les mêmes obligations ont été introduites pour les transports maritimes.

[5] *Enhanced Border Security and Visa Entry Reform Act of 2002,* voir également la *Immigration and Nationality Act.*

que pour les douanes US. Pour les passagers et les membres d'équipage partant des Etats-Unis, le transfert doit être effectué par voie électronique et terminé quinze minutes avant le décollage de l'avion, ce qui permet de mettre à jour ou de corriger le « manifeste » au plus tard dans les quinze minutes après le décollage de l'avion. *l'US Immigration and Naturalization Service* se réserve le droit de réclamer le retour de l'appareil aux Etats-Unis dans un délai d'une heure après son décollage, s'il le juge nécessaire.

Toutes les données doivent être transmises à une base de données centralisée[1] exploitée conjointement par les douanes US et *l'Immigration and Naturalization Service.* Les données seront alors partagées avec d'autres autorités fédérales et ne bénéficieront plus d'une protection spécifique[2].

Catégories de données transmises

L'APIS (acronyme pour *Advanced Passenger Information System :* système d'information anticipée sur les passagers) a connu des évolutions notables, évolutions se traduisant en particulier par une extension de la liste des données. Dès l'origine, les données requises ont été intrinsèquement associées au vol effectué, au visa ou à l'autorisation de séjour aux États-Unis ainsi qu'aux données d'identification telles qu'elles figurent dans les passeports.

La récente loi américaine sur la sécurité des frontières impose en particulier le transfert des données suivantes au *US Immigration Service* pour les vols à destination et au départ des Etats-Unis : identité, date de naissance, nationalité, sexe, numéro de passeport et lieu d'émission, pays de résidence, numéro de visa US, date et lieu d'émission (le cas échéant), numéro d'enregistrement d'étranger (le cas échéant), adresse aux États-Unis pendant le séjour ainsi que toute autre donnée estimée nécessaire pour l'identification des personnes transportées, la mise en œuvre des réglementations sur l'immigration ou pour protéger la sûreté et la sécurité nationales[3].

Outre ces données, le transfert sur demande, des données traitées dans les systèmes de réservation et de contrôle des départs (DCS) en particulier le *Passenger Name Record* (PNR) ou « dossier passagers » est actuellement requis [4]. Les données visées ne sont pas limitées aux passagers à destination des États-Unis et peuvent varier d'une compagnie à l'autre. Il peut s'agir[5] de données d'identification (nom, prénom, date de naissance, numéro de téléphone), du numéro de réservation PNR, de la date de réservation, le cas échéant de l'agence de voyage, d'informations reprises sur le ticket, de données financières (numéro de carte de crédit, date d'expiration, adresse de facturation, etc.), de l'itinéraire, de l'information du transporteur sur le vol (numéro de vol...), du siège occupé mais aussi de l'historique du PNR. Ce dernier peut reprendre les voyages effectués par le passé mais aussi des données religieuses ou ethniques (choix du repas...), l'affiliation à un groupe particulier, des données relatives à la résidence et aux moyens de contacter un individu (adresse e-mail, coordonnées d'un ami, lieu de travail....), des données médicales (assistance médicale nécessaire, oxygène, problèmes de vision, d'audition ou de mobilité ou tout autre problème dont la connaissance est nécessaire pour le bon déroulement du vol)

[1] *The Interagency Border Inspection System* (IBIS).
[2] Certaines de ces données pourraient être, le cas échéant, rendues publiques sur la base des législations d'accès à l'information détenue par le secteur public.
[3] Décision de l'« *Attorney General »,* en consultation avec le *Secretary of State et* le *Secretary of Treasury.*
[4] *Interim Rule (25 June 2002), Passenger Name Record Information Required for Passenger on Flights in Foreign Air Transportation* to *or from the United States.*
[5] Il est précisé explicitement que la liste est *« intended merely* to *be ilustrative of those data éléments to which Customs may request access ».*

ainsi que d'autres données liées par exemple aux programmes de fidélisation *(Frequent Fliers number)*[1].

En outre, pour les États participant au *« Visa Waiver Program »,* le transfert de données biométriques devrait être rendu obligatoire d'ici octobre 2004[2].

Sanctions

La non transmission des informations requises ou la transmission d'informations erronées ou incomplètes est assortie de lourdes sanctions, notamment la privation des droits d'atterrissage et des amendes pécuniaires très dissuasives[3].

Le groupe de travail se demande, à cet égard, si de telles mesures adoptées unilatéralement, peuvent être compatibles avec les conventions et les accords internationaux concernant le trafic et les transports aériens ainsi qu'avec la législation nationale applicable aux pays où les compagnies aériennes opèrent sur une base permanente.

Extension à d'autres pays

D'autres pays tels que le Canada, le Mexique [4], l'Australie, la Nouvelle-Zélande, l'Afrique du Sud et le Royaume-Uni on déjà mis ou prévoient de mettre en oeuvre des systèmes similaires répondant à leurs propres besoins.

Compatibilité avec la directive 95/46/CE

Application de la directive

Les données transmises par les compagnies aériennes sont des données relatives à des personnes physiques identifiées. Elles font l'objet d'un traitement par les compagnies aériennes sur le territoire de l'UE (collecte, enregistrement, modification, conservation, nouvelle modification, consultation, utilisation, communication...). Elles sont dès lors soumises à la protection offerte par la directive 95/46/CE.

En outre, l'évolution du système APIS suscite des préoccupations spécifiques exposées ci-après. La plupart dépassent les compétences des compagnies aériennes. Celles-ci se trouvent race à un dilemme dans la mesure où, d'une part, elles sont tenues de respecter la législation sur la protection des données transposant la directive 95/46/CE, et d'autre part, la législation américaine les oblige à transmettre les données sous peine d'amendes sévères.

Information des personnes concernées

Les personnes concernées devraient recevoir les informations nécessaires pour assurer un traitement loyal des données. Ces informations devraient préciser l'objet spécifique du traitement aux Etats-Unis ainsi que les destinataires des données.

L'article 13 de la directive 95/46/CE ne peut être invoqué valablement pour limiter cette obligation dans la mesure où le transfert est systématique et les catégories d'information requises ont dé à été partiellement rendues publiques aux Etats-Unis par la publication de la législation. Concrètement, ces informations devraient être fournies à la personne au moment où la collecte est effectivement réa-

---

[1] Ces données reprises dans les *Interim Rules* publiés par le *Department* of *Customs* sont néanmoins absentes de la loi 107-71.

[2] *Section 203 du Enhanced Border Security and Visa Entry Reform Act of 2002.*

[3] De l'ordre de 5 000 $ par erreur pour les *US. Customs* (par exemple, identité de passager ou autre critère en-dessous de la moyenne hebdomadaire acceptée] et 1 000 $ pour le *US Immigration and Naturalization Service* par identité incorrecte.

[4] Le Mexique va d'ailleurs communiquer aux ŝtats-Unis toutes les données obtenues sur les vols à destina tion du Mexique.

lisée et contenir en particulier l'objet spécifique du traitement aux États-Unis en incluant les destinataires des données[1].

Mesures de sécurité

Conformément à la directive 95/46/CE, les compagnies aériennes sont tenues de mettre en œuvre les mesures de sécurité appropriées pour protéger les données à caractère personnel. Cette obligation ne connaît aucune exception. Hors, il apparaît que les exigences techniques imposées par les Etats-Unis aux compagnies aériennes rendent les données vulnérables à des accès non-autorisés par des tiers.

Respect du principe de finalité

Compte tenu de l'évolution du système, la transmission des données personnelles telles que décrite au paragraphe ci-dessus, qui va au-delà de l'ensemble limité de données couramment communiquées par les passagers dans le cadre de l'organisation de leur voyage, ne peut pas être considérée comme compatible avec la finalité d'origine pour laquelle les données à caractère personnel ont été collectées par les compagnies aériennes ou agences de voyages, en particulier le respect de leurs obligations contractuelles vis-à-vis des passagers. L'article 6, paragraphe I, point b de la directive 95/46/CE interdit de traiter ultérieurement des données collectées pour des finalités déterminées, explicites et légitimes de manière incompatible avec ces finalités.

Au vu de leur nombre étendu, les données ne peuvent pas être considérées comme adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement, condition imposée à l'article 6, paragraphe 1, point c de la directive 95/46/CE.

Reste dès lors la possibilité de recourir à l'article 13 de la directive 95/46/CE, qui autorise les États membres à adopter des mesures législatives visant à limiter la portée de ces deux obligations pour autant que la limitation constitue une mesure nécessaire pour sauvegarder les intérêts énumérés à la même disposition (prévention et recherche d'infractions pénales, sécurité publique, etc.). Il serait bien entendu préférable que les États membres définissent une approche commune à cet égard.

Flux de données transfrontaliers

La directive 95/46/CE subordonne le transfert vers un pays tiers de données à caractère personnel à la condition que le pays tiers assure un niveau de protection adéquat. Le développement des systèmes APIS suscite une préoccupation dans cette perspective. Le traitement par les autorités fédérales américaines des données transmises par les compagnies aériennes ne répond pas à cette condition[2]. En raison de son champ d'application limité, la « sphère de sécurité » ne peut s'appliquer à la protection des transferts de données à destination d'autorités publiques.

Les exceptions énoncées à l'article 26 de la directive 95/46/CE ne semblent pas non plus pouvoir être utilisées.

Actuellement, l'application de l'exigence du consentement indubitable de la personne n'offre pas de solution satisfaisante car elle laisse subsister des préoccupations concernant de nombreux aspects. De toute façon, il ne semble pas que le consentement des passagers soit demandé, conformément à la législation en vigueur. La directive 95/46/CE définit le consentement comme une manifestation de

[1] Cela ne s'applique pas si les personnes concernées sont des suspects faisant l'objet d'une enquête.
[2] La loi sur la protection de la vie privée applicable aux autorités fédérales américaines ne protège que les données concernant les citoyens américains.

volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel fassent l'objet d'un traitement. Le consentement peut être compliqué à obtenir, essentiellement en raison des problèmes pratiques posés par la nécessité de communiquer clairement toutes les informations nécessaires aux passagers avant que ceux-ci ne fassent l'acquisition d'un billet. Nous sommes en présence de systèmes de réservation globaux qui permettent de réserver une place sur un vol allant de l'Union européenne aux États-Unis à partir de pratiquement n'importe quel pays dans le monde entier par des voies très différentes (différentes compagnies aériennes, agences de voyages, etc.). Les informations communiquées à la personne concernée doivent inclure les informations prévues aux articles 10 et 11 de la directive y compris, le cas échéant, l'absence de protection dans les pays tiers.

La nécessité du transfert pour l'exécution d'un contrat entre la personne concernée et le responsable du traitement peut difficilement être invoquée en raison de l'ampleur des données transmises. En effet, nombre de données transmises ne peuvent être considérées comme « nécessaires » à l'exécution du contrat. L'impossibilité matérielle pour les compagnies aériennes d'accomplir leurs engagements contractuels en raison notamment de la privation des droits, n'est pas suffisante à cet égard. Par ailleurs, cette exception est totalement inapplicable au transfert de données concernant les personnes ne voyageant pas vers les États-Unis.

De la même manière, il ne paraît pas non plus possible de se fonder sur la possibilité de transférer des données lorsque le transfert est nécessaire à la sauvegarde d'un intérêt public important. D'une part, le caractère de nécessité du transfert n'est pas établi. D'autre part, il ne paraît pas acceptable qu'une décision unilatérale d'un pays tiers pour des raisons d'intérêt public qui lui sont propres conduise au transfert régulier et massif de données protégées par la directive.

Enfin, il paraît difficile de considérer que le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.

La directive 95/46/CE autorise encore, par dérogation à la condition du niveau adéquat de la protection prévue par le pays tiers, que des données personnelles soient transférées lorsque le responsable du traitement (destinataire) offre des garanties suffisantes de protection des données.

Un dialogue pourrait dès lors utilement être engagé entre les États européens et les autorités américaines en vue de dégager une solution garantissant la protection adéquate des données transmises. Une approche commune au niveau européen serait appropriée.

Aspects spécifiques de la communication et de l'accès aux données du PNR traitées dans les systèmes de réservation automatisés ou dans les systèmes de contrôle des départs

Les remarques formulées sous ce point complètent les remarques du point précédent.

— Connexions électroniques directes des douanes américaines aux systèmes de réservation et de contrôle des départs

Au cas où il serait envisagé que les douanes américaines puissent accéder directement aux systèmes d'information sur le territoire européen et obtenir ou collecter des données plutôt que d'être les destinataires d'un flux de données transfrontalier classique, la directive pourrait être considérée dans sa totalité comme directement et totalement applicable à cette administration. L'article 4, paragraphe 1, pointe, prévoit l'applicabilité de la directive lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens

automatisés ou autres situés sur le territoire d'un État membre[1]. L'application de l'intégralité de la directive soulève toutefois nombre de questions.

— Données relatives aux personnes ne voyageant pas vers les États-Unis

Les données concernant les passagers ne voyageant par les vers les Etats-Unis ne sont pas pertinentes et ne peuvent donc être transmises sauf dans le cadre d'accords spécifiques dans le domaine de la justice et des affaires intérieures (assistance mutuelle).

— Données sensibles

Le PNR peut contenir des données susceptibles de révéler des origines raciales ou ethniques, des convictions religieuses ou d'autres données sensibles au sens de l'article 8 de la directive 95/46/CE. La directive 95/46/CE interdit en principe le traitement de données sensibles hors autorisation spécifique (consentement explicite à un tel traitement dans un but précis, données manifestement rendues publiques, etc.). Le recours au consentement crée de nombreux problèmes tels que décrits précédemment qui doivent être considérés avec d'autant plus d'attention que ces données présentent un caractère hautement sensible[2].

L'article 8, paragraphe 4 de la directive autorise les États membres ou les autorités de contrôle à prévoir d'autres exceptions, pour un motif d'intérêt public important et sous réserve de garanties appropriées. Moyennant le respect de ces conditions, les États membres pourraient dès lors autoriser le transfert des données sensibles contenues dans le PNR[3].

— Traitement de données par les systèmes de réservation et de contrôle des départs (DCS)

Par ailleurs, la question de l'accès au PNR, sur demande des autorités américaines, soulève d'emblée le problème de la légitimité du traitement de données effectué dans les systèmes de réservation et de contrôle des départs[4]. En particulier, seules les données adéquates pertinentes et non excessives au regard de la finalité poursuivie, peuvent être traitées et les données à caractère personnel ne devraient plus être traitées dans les systèmes de réservation dès lors qu'elles ne sont plus utilisées pour le voyage pour lequel elles ont été enregistrées.

---

[1] Le 20' considérant de la directive 95/46/CE indique que le fait que le traitement des données soit effectué par une personne établie dans un pays tiers ne doit pas faire obstacle à la protection des personnes prévue par la directive et que, dans ce cas, les traitements de données doivent être soumis à la loi de l'État membre dans lequel les moyens utilisés pour le traitement de données en cause sont localisés et, enfin, que des garanties doivent être prises pour que les droits et obligations prévus par la directive soient effectivement respectés. Dans un avis émis récemment, centré sur l'interprétation de la portée de l'article 4, paragraphe 1, point c de la directive (document de travail visant à déterminer l'applicabilité, au niveau international, de la législation européenne en matière de protection des données au traitement de données à caractère personnel sur internet par des sites web extérieurs à l'Union européenne — 30 mai 2002), le groupe de travail de l'article 29 a indiqué qu'il n'est pas nécessaire que le responsable dispose d'un contrôle complet sur les moyens mais bien qu'il détermine quelles données sont collectées, transférées, modifiées, etc. et dans quel but.

[2] Conformément à l'article 8, paragraphe 2, point a de la directive, la législation de l'Etat membre peut prévoir que l'interdiction du traitement des données visée à l'article 8, paragraphe 1 de la directive ne peut être levée par le consentement de la personne concernée.

[3] L'article 13 de la directive reste applicable.

[4] Voir la recommandation 1/98 sur les systèmes informatisés de réservation dans les transports aériens, qui mentionne également l'archivage des données pendant un certain temps pour le règlement des litiges et le traitement des données relatives aux clients fidélisés sur la base du consentement des personnes concernées. Le groupe de l'article 29 préconise en principe la conservation en ligne uniquement pour 72 heures et l'effacement dans un délai maximal de trois ans (avec accès limité aux demandes d'investigation), voire plus longtemps (mais conformément à une obligation légale).

Transfert de données biométriques

Le transfert de données biométriques est soumis aux dispositions de la directive 95/46/Œ. À noter que cette directive impose aux États membres de déterminer les conditions de traitement de tout identifiant de portée générale. Les identifiants biométriques permettent une identification unique des individus et pourraient être visés par cette disposition[1].

Conclusions

1) Le groupe de travail reconnaît le pouvoir discrétionnaire dont disposent les États souverains sur les informations qu'ils peuvent requérir des personnes souhaitant entrer sur leur territoire. Toutefois, les propositions actuelles concernant le système APIS qui ont été mises au point dans le contexte des atrocités commises par clés terroristes, conduiraient à la révélation disproportionnée et régulière, par les compagnies aériennes, d'informations soumises aux exigences de la directive *95/46/Œ.* Ces informations pourraient servir au traitement courant de questions en rapport avec l'immigration, les douanes, ainsi que, d'une façon plus générale, en rapport avec la sécurité nationale des États-Unis et pourraient être, au minimum partagées par toutes les agences fédérales américaines.

2) Compte tenu de l'évolution récente du système APIS, le groupe de travail est d'avis que l'application des exigences américaines crée des problèmes au titre de la directive *95/46/Œ.* La plupart des questions en jeu dépassent les compétences des compagnies aériennes et doivent être traitées par les États membres et le cas échéant par la Commission.

3) Sur le fond, le groupe de travail est d'avis que les transferts de données concernant les personnes ne voyageant pas vers les États-Unis doivent être exclus sauf dans le cas d'accords de coopération spécifiques dans le domaine de la justice et des affaires intérieures.

4) D'autres transmissions de données des systèmes de réservation et de contrôle des départs concernant les passagers et les membres d'équipage ne pourraient être envisagées que dans le cadre d'une législation des États membres.

Cette législation devrait prévoir que toute restriction nécessaire aux droits et obligations de la directive 95/46/CE soit conforme à l'article 13 de la directive et que des garanties soient accordées aux individus.

Une approche commune au niveau communautaire doit être recherchée.

5) Le transfert de données pouvant être jugées sensibles devrait être envisagé avec plus de réserve. Leur transfert suppose en outre que la preuve puisse être apportée :

— d'un motif d'intérêt public important dans le chef des États membres ;
— de garanties appropriées et ;
— une législation nationale ou une décision de l'autorité de contrôle est requise.

6) Lorsque l'accès direct des douanes et du service d'immigration américains aux données des systèmes de réservation et de contrôle des départs est également envisagé, ces autorités doivent s'engager à respecter la directive dans son ensemble.

7) Le système doit être négocié avec les autorités américaines. Les discussions devraient notamment porter sur une clarification et une définition des objectifs, des finalités et des destinataires ainsi que les catégories des données pouvant être transmises, eu égard à ces explications, ainsi que sur les conditions et garanties

[1] Le groupe de travail débat actuellement de la question des données biométriques.

entourant le traitement des données à caractère personnel, en particulier leur partage entre les autorités fédérales américaines (et, si tel est le cas, la limitation de leur accès aux autorités de police).

8) Le transfert de données personnelles des compagnies aériennes aux États-Unis devrait être envisagé de manière globale. Tout d'abord, il conviendrait de prendre en compte les autres transferts déjà existants ou envisagés actuellement vers les États-Unis. Il serait particulièrement nécessaire d'intégrer le concept du troisième pilier. Fondamentalement, les transferts de données à destination, d'autorités publiques d'un État tiers pour des raisons liées à l'ordre public de cet État devraient être appréhendés dans le contexte des mécanismes de coopération instaurés dans le troisième pilier (coopération judiciaire et policière). Ces mécanismes devraient d'ailleurs aller de pair avec des garanties de protection des données transférées[1]. Il apparaît important d'éviter un contournement *via* le premier pilier de ces mécanismes normaux de coopération instaurés dans le troisième pilier. Enfin, la solution dégagée pour le transfert de données vers les États-Unis devrait pouvoir servir de référence en ce qui concerne les transferts par APIS vers d'autres pays tiers.

INTERNET

Les services d'authentification en ligne [Document de travail — 29 janvier 2003]

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 ;

Vu les articles 29 et 30, paragraphe 1, point a et paragraphe 3 de la directive précitée ;

Vu son règlement et notamment les articles 12 et 14 de ce dernier ;

A adopté le présent document de travail :

Introduction : l'expansion des services d'authentification en ligne

Le développement des services d'authentification en ligne a modifié le paysage de l'internet. De plus en plus de sites web proposent ou demandent à leurs visiteurs de s'identifier, par exemple parce qu'ils fournissent des informations sécurisées, offrent la possibilité d'enregistrer les préférences de l'utilisateur, proposent un service payant ou doivent livrer des produits. Tous ces sites exigent de la part de l'utilisateur qu'il s'identifie, le plus souvent via son adresse électronique associée à un mot de passe.

La combinaison nom d'utilisateur/mot de passe peut poser quelques problèmes aux fournisseurs de services :

— les utilisateurs ont tendance à oublier leur mot de passe. Un nombre croissant d'appels ou de courriers électroniques parvenant aux services d'assistance concerne

[1] Des données à caractère personnel sont exportées par les États membres dans le contexte de la coopération policière et judiciaire. Des données sont transférées par Europol pour enquêter sur les événements du 11 septembre 2001 sur la base d'une procédure d'exception et des discussions sont en cours pour établir une coopération sur une base stable en conformité avec les exigences de la Convention Europol (article 18). Voir aussi la décision Eurojust (article 27). Voir enfin les négociations menées actuellement sur la base de l'article 38 du traité.

l'oubli de ce mot de passe. Pour les sites web, les coûts liés à la réactivation des mots de passe deviennent de plus en plus importants ;
— de plus en plus d'utilisateurs se connectent à l'internet par des moyens différents mais pour avoir accès à des services identiques. Les modes de connexion peuvent re poser sur des configurations techniques différentes — connexion à partir d'un ordina teur personnel ou d'un téléphone mobile WAP — mais de plus en plus, l'on se connecte à l'internet à partir d'ordinateurs personnels différents, situés dans des cy bercafés ou des bibliothèques publiques, ce qui implique que les utilisateurs doivent absolument se souvenir de leur mot de passe ;
— enfin, certains utilisateurs n'aiment pas saisir leur nom d'utilisateur et leur mot de passe car ils estiment que cela nuit à la convivialité. Les utilisateurs ont tendance à li miter leurs efforts et se contentent donc de saisir des mots de passe succincts qui ne sont pas fiables et qui sont souvent partagés sur un grand nombre de sites web.

Toute solution aux trois problèmes précités requiert de la part de l'utilisateur qu'il délègue une partie du processus d'authentification. À l'heure actuelle, il existe quatre possibilités :
— la gestion des mots de passe est déléguée au logiciel de navigation sur internet de l'ordinateur personnel de l'utilisateur, comme c'est le cas du gestionnaire de mots de passe Mozilla ;
— la gestion des mots de passe est déléguée à un serveur « proxy » sur l'internet, éventuellement mis à disposition par le fournisseur de services internet (FSI) ;
— l'authentification est prise en charge par une tierce partie, laquelle utilise un proto cole d'authentification spécifique. C'est le cas du système Microsoft NET Passport ;
— le service d'authentification est pris en charge par une partie contractante au sein d'un « cercle de confiance ». Un protocole spécifique est utilisé, comme par exemple pour Liberty Alliance.

Ces possibilités sont examinées dans les paragraphes suivants :

1) Un gestionnaire de mots de passe intégré à l'ordinateur personnel

Posséder un gestionnaire de mots de passe intégré au navigateur internet ne résout qu'une partie du problème. L'utilisateur n'a plus à saisir de mot de passe et, de ce fait, il ne risque pas de l'oublier. Toutefois, le problème des utilisateurs mobiles qui se connectent à partir de différents ordinateurs personnels n'est pas réglé.

La situation est assez simple au regard de la protection des données à caractère personnel. Tous les logiciels concernés sont installés sur l'ordinateur personnel de l'utilisateur et sont sous le contrôle de celui-ci. Aucune entreprise extérieure ne contrôle les données. Le système demande à l'utilisateur s'il souhaite que les informations soient intégrées à la base de données du gestionnaire de mots de passe. Le gestionnaire de mots de passe saisit le mot de passe mais ne l'envoie cependant pas tant que l'utilisateur n'a pas donné son consentement. Du point de vue de la sécurité, il est nécessaire de prendre des mesures adéquates pour s'assurer que le stockage des données soit protégé contre le piratage.

2) Utilisation d'un serveur « proxy »

Dans ce cas, au lieu d'utiliser un gestionnaire de mots de passe installé sur l'ordinateur personnel de l'utilisateur (le navigateur), on a recours à une fonctionnalité similaire intégrée à un serveur « proxy » sur l'internet. Cette fonctionnalité est comparable à la technologie mieux connue du « proxy » anonyme. Un serveur « proxy » peut servir à de nombreux utilisateurs ; dès lors, un mot de passe doit être enregistré par utilisateur et par site cible. Il faut que l'utilisateur ait confiance dans le processus d'enregistrement, une confiance exprimée d'ailleurs de façon explicite par l'utilisateur dans la mesure où la décision de recourir à un serveur « proxy » est prise en

toute conscience (il n'y a pas de service par défaut). L'utilisateur doit s'identifier sur le serveur « proxy » s'il veut utiliser ses mots de passe. Une fois l'utilisateur dûment identifié, le serveur « proxy » offre à ce dernier les mêmes avantages que le gestionnaire de mots dépasse intégré. L'avantage du serveur « proxy » est qu'il est accessible à partir de différents ordinateurs personnels et/ou à autres dispositifs.

Les serveurs « proxy » ne devraient jamais divulguer à une tierce partie des informations relatives à l'utilisateur sans le consentement de celui-ci. En le faisant, ils perdent la confiance de leurs clients et donc leur raison d'être. Normalement, un contrat doit être conclu entre le fournisseur de services « proxy » et le client. Ce service peut probablement être payé par d'autres sources que la publicité, éventuellement en combinaison avec le service fourni par le FSI.

3) Services d'authentificafion en ligne utilisant des protocoles spéciaux

Aucune des solutions décrites ci-dessus ne nécessite une modification du site web du fournisseur de services. Une autre possibilité serait de procéder à l'authentification en recourant à un protocole spécial d'authentification. Pour ces protocoles, l'architecture de base reste la même. Il y a en effet toujours trois parties : un utilisateur final, un fournisseur de services et un fournisseur de services d'authentification. Avant de bénéficier des services du fournisseur de services, l'utilisateur final voit son identité vérifiée par le fournisseur de services d'authentification. Le fournisseur de services se fie au fournisseur de services d'authentification et accepte d'accueillir un utilisateur.

L'architecture de NET Passport repose sur un serveur d'authentification unique, administré par Microsoft. Le « Passport » contient des données d'identification et d'authentification ainsi que des données relatives au profil de l'utilisateur. À l'avenir, l'on s'attend à ce que ces deux séries de données soient de plus en plus dissociées. L'utilisateur qui se connecte à Passport se voit attribuer un identifiant unique ou PUID. Si l'utilisateur souhaite se connecter à un fournisseur de services, il donne l'instruction au serveur Passport de transmettre son PUID sous une forme lisible par ledit fournisseur de services (actuellement par un procédé de cryptage symétrique).

Le système Liberty Alliance repose sur un modèle fédéré. Un utilisateur peut fédérer son compte entre deux fournisseurs de services. Une fois ce compte fédéré, un fournisseur de services acceptera d'accueillir l'autre fournisseur de services, l'autre fournisseur de services agissant en tant que responsable de la procédure d'authentification.

Conscient de l'expansion des services d'authentification en ligne, le groupe de travail a décidé il y a quelques mois d'examiner l'impact de ces systèmes sur la protection des données[1]. Conscient également de l'importance de mécanismes d'authentification sûrs pour garantir l'intégrité et la sécurité de certaines transactions électroniques, en particulier celles impliquant des paiements en ligne, le groupe de travail souhaite souligner que le développement de ces services doit respecter les principes de base de la protection des données en vertu des dispositions établies dans la directive européenne en la matière[2] ainsi que dans les réglementations nationales transposant cette directive.

[1] *Cf.* WP 60, document de travail — Premières orientations du groupe de travail « Article 29 » concernant les services d'authentification en ligne, adopté le 2 juillet 2002.

[2] *Journal officiel* n° L 281 du 23 novembre 1995, p. 31, disponible à l'adresse suivante : http : //europa.eu.int/comm/internal_market/en/dataprot/index.htm

Étude de cas 1 : Microsoft .NET Passport

. NET Passport étant une initiative particulièrement importante à l'heure actuelle dans ce domaine, le groupe de travail a tout d'abord procédé à une première étude de ce système au printemps 2002[1]. Après une première analyse, le groupe de travail est arrivé à la conclusion que, bien que Microsoft ait mis en place diverses mesures pour assurer la protection des données, un certain nombre d'éléments du système .NET Passport soulèvent des problèmes juridiques et nécessitent donc un examen approfondi.

Au cours des mois suivants, le groupe de travail a entamé un dialogue avec Microsoft afin d'obtenir une meilleure compréhension du fonctionnement du système, de discuter des différents problèmes posés par celui-ci et, plus particulièrement, d'évaluer si les principes européens de protection des données sont correctement appliqués et, le, cas échéant, d'identifier les éléments du système qui requièrent des modifications. À la suite de ce dialogue très riche et très ouvert, Microsoft s'est engagé à apporter des modifications au système, qui devraient fortement améliorer celui-ci au regard de la protection des données.

L'engagement de Microsoft de mettre en œuvre toutes les mesures discutées avec le groupe de travail a été expliqué dans plusieurs lettres adressées au président du groupe de travail, le professeur Rodotà, un calendrier ayant même été élaboré précisant les différents délais retenus pour la mise en œuvre de chaque mesure. Les mesures à prendre étant de natures différentes, leur mise en œuvre s'effectuera nécessairement sur une période plus ou moins longue. Certaines des mesures approuvées, comme la révision de la déclaration de confidentialité de .NET Passport et l'ajout d'informations sur les pages relatives à la procédure d'enregistrement, sont simples et peuvent être rapidement mises en oeuvre. D'autres, comme la nouvelle procédure d'information décrite ci-dessous, supposent un recodage considérable du service .NET Passport et demandent donc plus de temps pour être mises en œuvre.

Le groupe de travail a pris acte de l'échéancier présenté par Microsoft pour répondre aux préoccupations du Groupe. Cet échéancier comporte trois types de délai qui seront indiqués entre parenthèses après chaque mesure : premier délai (0-4 mois), second délai (4-8 mois), troisième délai (8-18 mois . Entre-temps, certaines des mesures examinées ont été mises en œuvre et seront dès ors mentionnées comme faisant partie de la pratique actuelle.

Brève description du système Microsoft. NET Passport

.NET Passport est un service d'authentification sur l'internet permettant de se connecter aux différents sites web participants en s'identifiant une seule fois *(single sign-in),* cela afin de faire gagner du temps aux utilisateurs et de leur éviter de ressaisir à chaque fois leur nom d'utilisateur et leur mot de passe lorsqu'ils naviguent sur l'internet. Il ne s'agit ni d'un service d'autorisation ni d'un service d'identification mais bien d'un service d'authentification visant à authentifier un utilisateur une seule fois et en toute sécurité en vérifiant ses données d'identification[2].

Le système a été créé en 1999 et a été rebaptisé .NET Passport durant l'été 2000. Actuellement, plus de 250 millions de comptes ont été ouverts à travers le

[1] *Cf.* WP 60, document de travail — Premières orientations du groupe de travail « Article 29 » concernant les services d'authentification en ligne, adopté le 2 juillet 2002.

[2] L'on doit garder à l'esprit qu'outre la directive relative à la protection des données personnelles, d'autres directives peuvent également trouver à s'appliquer à ce type de services, notamment les directives sur le commerce électronique ou sur la signature électronique.

monde (un utilisateur peut avoir plusieurs comptes, a fortiori s'il possède plusieurs comptes Hotmail). Plus de 40 millions décomptes ont été ouverts par des résidents de l'Union européenne.

Il existe plusieurs façons d'obtenir un Passport :
— en s'inscrivant sur le site www.passport.net ;
— en s'inscrivant sur l'un des sites participants ;
— en souscrivant à un compte de messagerie Hotmail.

Près de 87 % des utilisateurs se sont inscrits *via* un site participant ou *via* Hotmail, pas directement par le biais du site de Microsoft. Près de 120 millions de comptes appartiennent à des titulaires de comptes de messagerie Hotmail. Hotmail est un service de messagerie électronique utilisé partout dans le monde et entièrement géré par Microsoft et d'autres sociétés contrôlées par Microsot. Un grand nombre de comptes appartiennent par ailleurs à des utilisateurs du service Windows Messenger (MSN).

Les données personnelles collectées peuvent actuellement être classées dans trois catégories prédéterminées :

1) Les informations minimales : nom d'utilisateur (adresse électronique) et mot de passe.

2) Données d'identification : question et réponse secrètes, qui sont nécessai res en cas d'oubli du mot de passe, numéro de téléphone et numéro d'identification personnel (PIN), code de sécurité et trois questions et réponses additionnelles.

Ces informations ne sont pas reprises dans le profil et ne sont pas communiquées à d'autres sites.

3) Données exhaustives relatives au profil : elles comprennent, outre les informations susmentionnées, le nom, le prénom, le fuseau horaire, le sexe, la date de naissance, la profession et l'accessibilité de la personne.

Les sites participants peuvent collecter directement auprès de l'utilisateur des informations supplémentaires aux fins de leur traitement ultérieur. À l'heure actuelle, soixante-neuf sites externes participants (non liés à Microsoft) proposent le service .NET Passport, vingt-deux d'entre eux se situant sur le territoire de l'EEE.

Problèmes juridiques en jeu et résultat du dialogue avec Microsoft

Dans son document de juillet 2002, le groupe de travail a mis en évidence un certain nombre de problèmes nécessitant un examen approfondi. Dans les paragraphes qui suivent, chacun de ces problèmes sera passé en revue. Le résultat du dialogue avec Microsoft sera également examiné pour chaque problème particulier mis en évidence.

D'un point de vue général, il convient de préciser qu'outre les mesures spécifiques qui seront décrites dans les paragraphes qui suivent, Microsoft a décidé de modifier la procédure d'information applicable au système .NET Passport. En principe, le service sera recodé en vue d'établir une nette distinction entre la création d'un compte .NET Passport et le stockage d'informations personnelles dans le profil Passport. Cette nouvelle procédure d'information, qui sera expliquée de manière détaillée dans le chapitre consacré aux questions de proportionnalité, devrait avoir un impact positif sur la loyauté de la collecte et du traitement des données personnelles des utilisateurs. Le groupe de travail s'en félicite.

Les *informations fournies aux personnes concernées au moment de la collecte des données, de leur traitement ultérieur ou de leur transfert à une tierce partie, située éventuellement dans un pays tiers*

Lorsqu'il a commencé à se pencher sur le fonctionnement du service .NET Passport, le groupe de travail s'est trouvé tout d'abord confronté au problème du manque d'informations claires et transparentes concernant ce système. Une partie de la documentation d'information existante concernant ce système était souvent peu claire, omettait de fournir les renseignements les plus fondamentaux liés à la protection des données (identité du responsable du traitement, finalité du traitement, droits des personnes concernées, destinataires des données, conditions requises pour garantir un traitement équitable) et comportait parfois des déclarations contradictoires.

Deux points ont particulièrement inquiété le groupe de travail, à savoir le manque d'informations précises à propos du transfert de données personnelles vers un pays tiers et l'absence de renseignements quant au lien entre Hotmail et Passport.

Entre-temps, Microsoft s'est engagé à prendre les mesures suivantes en vue de répondre aux inquiétudes soulevées par le groupe de travail à cet égard :

— Comme le recommande le groupe de travail « Article 29 » dans sa recommandation 2/2001[1], Microsoft proposera un *« pop up » (prompt box)* conte nant les informations requises par l'article 10 de la directive, le tout présenté de manière très accessible et conviviale. Un lien vers le *« pop up »* sera affiché pour les utilisateurs qui s'identifient comme résidents dans l'Union européenne dès leur entrée sur la page d'enregistrement où ils indiquent leur pays de résidence. Les utilisateurs qui cliquent sur ce lien verront alors apparaître le *« pop up »* dans une fenêtre séparée. Cette fonctionnalité sera disponible en avril 2003 au plus tard.

— Les utilisateurs seront informés, lorsqu'ils s'inscrivent sur un site partici pant, du pays dans lequel ce site est situé (8-18 mois) et pourront accéder, *via* le *« pop up »,* à un lien vers la page web de la Commission reprenant la liste des pays dont les réglementations en matière de protection des données ont été déclarées conformes aux normes de l'UE en la matière (4-8 mois).

— Microsoft informera les utilisateurs de l'UE, *via* le *« pop up »,* de la durée de conservation des données d'enregistrement (actuellement 90 jours au maximum) (0-4 mois).

— Au tout début de la procédure, les utilisateurs seront clairement informés sur la manière d'ouvrir un compte .NET Passport sans avoir à introduire leur adresse électronique réelle, une fonctionnalité que le groupe de travail a recommandé d'inclure à plusieurs reprises. En outre, les utilisateurs seront prévenus des limites de l'ouverture de comptes sous un pseudonyme de manière à pouvoir prendre une déci sion en connaissance de cause (8-18 mois).

— Microsoft s'est engagé à actualiser en même temps toutes les versions lin guistiques de la déclaration de confidentialité de .NET Passport, excepté là où le contexte local exige une modification immédiate dans une version linguistique parti culière. Dans ces cas, qui ne devraient se présenter que très rarement, Microsoft insé rera une mention dans les autres versions linguistiques de la déclaration de confidentialité précisant qu'elles seront mises à jour dans peu de temps (0-4 mois).

— Microsoft s'est engagé à prendre une série de mesures visant à garantir que lorsque des utilisateurs ouvrent un compte Hotmail, ceux-ci soient également

[1] Recommandation 2/2001 concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne, adoptée le 17 mai 2001, WP 43.

informés de l'ouverture simultanée d'un compte Passport (pratique actuelle) et que lorsque des utilisateurs ouvrent un compte Hotmail, ceux-ci soient également informés de la nécessité d'obtenir un compte Passport pour accéder à Hotmail et de l'obligation de clôturer leur compte Hotmail pour pouvoir résilier leur compte Passport (0-4 mois).

La valeur et la qualité du consentement donné par les personnes concernées à ces opérations

Après une première analyse du système, le groupe de travail s'est posé des questions sur la validité et la qualité du consentement autorisant le traitement conformément aux dispositions de l'article 2h de la directive[1]. En d'autres termes, le groupe de travail n'était pas convaincu que le consentement donné par les utilisateurs fût suffisamment informé, libre et spécifique, notamment en ce qui concerne les utilisateurs s'inscrivant *via* Hotmail et la transmission de données à caractère personnel vers des sites participants.

Comme il vient d'être expliqué ci-dessus, Microsoft a pris et s'est engagé à prendre toute une série de mesures visant à garantir une information loyale des utilisateurs. Par ailleurs, s'agissant de la possibilité pour les utilisateurs de décider de fournir ou non des informations à caractère personnel au système Passport, la nouvelle procédure d'information permettra aux utilisateurs de communiquer leurs données personnelles à un site participant sans les stocker sur leur profil Passport et d'obtenir un compte Passport sous un pseudonyme sans avoir à fournir de renseignements personnels supplémentaires (8-18 mois).

En ce qui concerne les utilisateurs d'Hotmail, outre l'amélioration de l'information, des mesures sont prises en vue d'avertir clairement les utilisateurs qu'en ouvrant un compte Hotmail, leurs données personnelles seront utilisées pour la finalité d'envoi de publicités (0-4 mois). Pour ce faire, sur la page d'enregistrement aux services Hotmail, il sera clairement expliqué aux utilisateurs qu'en acceptant les conditions d'utilisation d'Hotmail, ceux-ci acceptent de recevoir de la publicité de la part d'Hotmail. Comme avec n'importe quel site participant, les utilisateurs qui s'inscrivent à .NET Passport *via* le site d'Hotmail auront le choix de ne divulguer leurs données personnelles qu'à Hotmail sans les stocker dans leur profil .NET Passport (8-18 mois).

Le groupe de travail a également discuté avec Microsoft quant à la possibilité pour les utilisateurs d'Hotmail de choisir de ne pas recevoir de publicités personnalisées. Microsoft a expliqué que les utilisateurs possédant un compte Hotmail pouvaient choisir gratuitement de ne pas recevoir de publicités personnalisées mais qu'ils devaient pour cela fermer leur compte Hotmail. Les utilisateurs ne peuvent pas détenir un compte Hotmail sans recevoir de publicités personnalisées, car ce sont précisément les recettes dérivées de ces publicités ciblées qui permettent de proposer l'ouverture d'un compte Hotmail à titre gratuit.

Le groupe de travail doute encore de la conformité de cette pratique avec la législation européenne et poursuivra à l'avenir sa réflexion sur ce problème. Il considère toutefois qu'il s'agit là d'un problème spécifique, à savoir la pratique suivie par plusieurs sociétés en vertu de laquelle la prestation d'un service est liée à l'obligation pour l'utilisateur d'accepter que ses données soient utilisées à des fins publicitaires, sans qu'il ait la possibilité de s'y opposer. Ce problème, qui se distingue de la question particulière des services d'authentification en ligne qui fait l'objet du présent document de travail, sera abordé ultérieurement dans un contexte plus large.

[1] On entend par « consentement de la personne concernée », toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Pour ce qui est du consentement des utilisateurs vis-à-vis des sites participants, la nouvelle procédure d'enregistrement permettra aux utilisateurs d'obtenir un Passport ne reprenant que le nom d'utilisateur et le mot de passe, et cela en dissociant la création d'un compte Passport de la décision de communiquer ses données personnelles au site participant ou de les stocker dans le profil (8-18 mois). Les utilisateurs seront informés de la possibilité d'obtenir un Passport *via* le site Passport en n'introduisant qu'un nom d'utilisateur et qu'un mot de passe. Ils seront également avertis qu'en s'inscrivant sur un site participant, ils peuvent être obligés de fournir d'autres informations (informations reprises dans un *« pop up »* dans un délai de 4 à 8 mois). Une nouvelle fonctionnalité sera également ajoutée afin de permettre aux utilisateurs de décider, site par site, s'ils acceptent de partager ou non les données reprises dans leur profil. Le profil des utilisateurs sera reconfiguré de façon à permettre à ces derniers de compléter les champs de leur choix et de ne rien indiquer dans d'autres (8-18 mois).

La nouvelle procédure d'information permettra également aux utilisateurs, chaque fois qu'ils s'inscrivent sur un site participant, de réviser les données de leur profil, de les modifier, de décider de sauvegarder ces modifications dans leur profil Passport et de déterminer quelles informations ils souhaitent transmettre au site en question (8-18 mois).

La proportionnalité et la qualité des données collectées et stockées par .NET Passport, puis transmises aux sites affiliés

Le groupe de travail s'est inquiété de la quantité de données collectées *via* Passport, en particulier les données relatives au profil de l'utilisateur, ainsi que du fait qu'après avoir créé un compte .NET Passport, la personne concernée — si elle a coché les cases destinées à autoriser le partage des données — risque de voir ses données personnelles transmises à l'ensemble des sites participants qu'elle visite et auxquels elle s'inscrit, indépendamment du fait que ces informations soient nécessaires ou non pour le site en question. Au moment de la réalisation de la première étude du système, l'utilisateur n'avait pas la possibilité d'autoriser la transmission d'une partie des données, les informations contenues dans le profil étant considérées comme un ensemble indissociable.

La nouvelle procédure d'information à mettre en place par Microsoft dissociera clairement la création d'un compte .NET Passport de la décision de l'utilisateur de communiquer ses informations personnelles au site participant et, éventuellement, à .NET Passport. Les utilisateurs seront libres de choisir, sur la base d'un consentement *(opt-in),* de stocker ou non sur leur profil .NET Passport les informations qu'ils acceptent de communiquer au site sur lequel ils s'inscrivent. Lorsqu'un utilisateur, ayant choisi de stocker ces informations sur son profil .NET Passport, visite d'autres sites participants, il aura la possibilité de modifier ou de supprimer ces informations, champ par champ, avant de les communiquer au site participant. L'utilisateur sera également libre, sur la base d'un consentement *(opt-in),* de sauvegarder ces modifications ou suppressions dans son profil .NET Passport (8-18 mois).

Ces changements, outre le fait que l'utilisateur puisse décider de ne pas utiliser son adresse électronique réelle dans certains cas, répondront, une fois mis en œuvre, aux préoccupations du groupe de travail, mais le groupe de travail souhaite continuer à surveiller l'évolution de ces questions, en particulier en prenant en compte le rôle de Microsoft en tant que responsable du traitement ainsi que toute autre information valable communiquée par les utilisateurs.

Les règles de protection des données appliquées par les sites web affiliés à .NET Passport

Le groupe de travail s'est également inquiété du manque de clarté concernant le niveau de protection assuré par les sites participants.

Lors de ses discussions avec le groupe de travail, Microsoft a précisé qu'il ne contrôlait pas les règles appliquées par les sites participants en matière de protection des données mais que les contrats conclus avec ces sites exigeaient un certain nombre de garanties à cet égard. Par exemple, les sites en question sont tenus d'appliquer une politique de protection de la vie privée qui soit effective, facilement accessible et conforme aux pratiques en vigueur dans le secteur, de prendre des mesures de sécurité adéquates, de respecter la législation applicable et de ne pas utiliser les données pour d'autres finalités que celles de la fourniture de services spécifiques sans le consentement de l'utilisateur.

Microsoft s'est engagé à prendre un certain nombre de mesures additionnelles :

— Revoir la déclaration de confidentialité de manière à indiquer clairement que Microsoft ne contrôle pas les pratiques des sites participants en matière de protection des données (0-4 mois).

— Microsoft encouragera les sites participants à adhérer à TRUSTe, BBBOnLine, ou à des services similaires (0-4 mois).

— Les sites participants auront la possibilité — à la fois sur la page de collecte des informations personnelles et, de manière plus détaillée, par le biais d'un lien figurant sur cette page — d'informer les utilisateurs des finalités de l'utilisation de leurs données, des destinataires et des durées de conservation de celles-ci (8-18 mois).

Il convient de préciser en tous les cas que, mis à part le rôle joué par Microsoft dans le système .NET Passport, tous les sites participants doivent être considérés comme responsables de leurs propres opérations de traitement. Ils sont dès lors personnellement responsables du respect de la législation de protection des données à caractère personnel au regard de ces opérations de traitement.

La nécessité et les conditions d'emploi d'un identifiant unique

Dès qu'il a commencé à étudier le système Passport, le groupe de travail s'est inquiété de l'utilisation par .NET Passport d'un identifiant unique — le PUID — pour chaque utilisateur.

L'identifiant unique du système Passport (PUID) est créé dès l'inscription et reste valide pendant toute la durée de vie du compte. Il s'agit d'une chaîne de 64 bits comprenant deux parties : 16 bits destinés à identifier le centre de données à partir duquel le code est généré et 48 bits destinés à identifier un compte spécifique. La principale exigence pour la génération du PUID est qu'il soit unique. Le PUID ne repose pas sur une information fournie par le titulaire du compte et aucune information concernant le titulaire du compte ne peut être déduite du PUID.

Le PUID sert avant tout à offrir la possibilité de répertorier les identifiants dans la base de données propre à chaque site. À lui seul, le PUID ne permet pas l'ouverture d'une session ni l'accès à des informations sur le profil de l'utilisateur. Seul un ticket d'authentification correctement créé (comprenant le PUID), crypté dans la clé attribuée au site participant, permet d'ouvrir une session. Tout utilisateur peut se voir attribuer un ou plusieurs PUID dans la mesure où un PUID est créé pour chaque compte Passport et que les utilisateurs peuvent ouvrir plus d'un compte Passport.

La principale inquiétude du groupe de travail était que l'utilisation du PUID permette aux sites participants de communiquer entre eux des informations concernant les utilisateurs de .NET Passport et de créer des profils d'utilisateurs. Les contrats conclus entre Microsoft et les sites affiliés interdisent la vente de registres PUID à des tiers ou le croisement de données entre sites *(cross-site linking)* sans le consentement de l'utilisateur, et limitent fortement l'utilisation du PUID. Toutefois, un risque n'est

jamais exclu dès lors qu'il est techniquement possible qu'il survienne. Le groupe de travail a soulevé un autre problème : la possibilité pour les utilisateurs d'avoir accès à leur propre PUID.

Sur ce second point, Microsoft a accepté que les utilisateurs puissent avoir accès à leur PUID sur demande (8-18 mois). Le groupe de travail souhaiterait attirer l'attention sur le délai excessivement long avant lequel il ne serait pas possible d'exercer son droit d'accès au PUID. Même si cet accès n'est pas possible en ligne, d'autres moyens doivent dès maintenant être offerts aux utilisateurs pour exercer ce droit.

Microsoft et les membres de la *task-force* « internet » ont beaucoup discuté sur la nécessité même d'avoir recours à un identifiant unique. Microsoft comprend les craintes du groupe de travail et a accepté de continuer à étudier des architectures d'identification alternatives pour .NET Passport.

Il a été convenu avec Microsoft de poursuivre ultérieurement le débat sur cette question de façon à voir si une alternative viable peut être trouvée.

L'exercice des droits des personnes concernées

Le groupe de travail a fait part de son inquiétude quant aux problèmes relatifs aux droits des personnes concernées et, plus particulièrement, à la difficulté de se désabonner du service Passport.

Lors de ses échanges de vues avec le groupe de travail, Microsoft a reconnu que des problèmes s'étaient présentés par le passé et a accepté de mettre en œuvre plusieurs mesures facilitant l'exercice de leurs droits par les utilisateurs :

— Faire figurer dans le *« pop up »* un résumé clair et lisible des informations requises par l'article 10 de la directive, ainsi que des informations relatives aux droits des personnes concernées (avril 2003 au plus tard).

— Informer les utilisateurs, dans la déclaration de confidentialité et dans le courrier électronique d'introduction, qu'ils doivent faire parvenir leurs questions et requêtes à l'adresse électronique suivante : passpriv@microsoft.com (pratique actuelle et 0-4 mois).

— Répondre aux questions et requêtes des utilisateurs de Passport dans leur langue, à condition que cette langue figure parmi celles dans lesquelles Passport est disponible (0-4 mois).

Depuis septembre 2002, les utilisateurs peuvent clôturer facilement leur compte .NET Passport en se rendant sur le site www.passport.net et en cliquant sur le lien « Services aux utilisateurs ». L'utilisateur sera ensuite guidé à travers les différentes étapes qui le conduiront à clôturer son compte Passport personnel. Pour les comptes créés sur le site www.passport.net, la procédure est totalement automatisée. L'utilisateur se retrouve face à une page qui décrit les conséquences de la fermeture du compte et doit cliquer sur un bouton pour le clôturer. Pour les comptes créés *via* Hotmail, la procédure est assez similaire : l'utilisateur est dirigé vers le site d'Hotmail où se trouve la page expliquant la procédure de à suivre pour fermer le compte.

Les risques en matière de sécurité liés à ces opérations

Le groupe de travail a également examiné les éventuels risques en matière de sécurité, notamment ceux liés à la concentration de données dans deux grandes bases de données, que peut comporter le système. Ces inquiétudes ont également été inspirées par le fait que Microsoft a toujours été l'une des cibles privilégiées des pirates informatiques.

Le groupe de travail a pris acte de ce que Microsoft a mis en place un « Programme de sécurité des systèmes d'information » *(Information Security Program)*

suite au *Consent Order* prononcé par la *Federal Trade Commission* en 2002. Les principales exigences sont :

— La mise en œuvre de garanties *ad hoc* sur les plans administratif, tech nique et physique, ainsi que d'une politique de sécurité remaniée, reposant sur la norme ISO 17799. Les procédures d'exploitation standard pour chaque groupe d'importance seront modifiées au besoin en vue de garantir la conformité par rap port au « Programme de sécurité des systèmes d'information ». Ces procédures seront actualisées si nécessaire, en fonction du développement technologique et éco nomique.

— La désignation d'un ou de plusieurs employé(s) responsable(s) du « Pro gramme de sécurité des systèmes d'information » et chargé(s) de le coordonner. Les principales parties prenantes au sein de tous les groupes impliqués aideront à l'éla boration et à la mise en œuvre de procédures d'exploitation standard appliquant le « Programme de sécurité des systèmes d'information ».

Plusieurs autres initiatives sont en cours de développement ou de finalisation, parallèlement à la mise en œuvre du nouveau « Programme de sécurité des systèmes d'information ». Parmi celles-ci, citons :

— Formation à la sécurité destinée aux équipes responsables du développe ment des opérations et des applications.

— Procédures d'intervention et de signalisation progressive en cas d'incidents.

— Création d'une cellule de supervision de la sécurité.

Conclusion

Le groupe de travail se félicite des mesures très importantes que Microsoft a prises et s'apprête à prendre dans les prochains mois afin de garantir et de renforcer la conformité du système .NET Passport avec la directive européenne sur la protection des données. Il est évident que le groupe de travail surveillera de très près l'évolution du système au cours des prochains mois, afin de voir comment les mesures annoncées par Microsoft seront appliquées.

Le groupe de travail prend également note des préoccupations émises par certaines ONG concernant l'installation d'un système centralisé de stockage de données personnelles. Le groupe de travail continuera à suivre ces questions, y compris en ce qui concerne les caractéristiques de sécurité de ce système.

Ainsi, en raison de la nature évolutive du service .NET Passport, des éventuels développements concernant sa future architecture et de la nécessité de poursuivre la réflexion sur un certain nombre des problèmes précités — en particulier en ce qui concerne le PUID —, le groupe de travail continuera à étudier le déploiement du système ainsi que son développement futur, au besoin en dialoguant avec Microsoft. Microsoft s'est engagé à rapporter au groupe de travail les mesures prises concernant le système .NET Passport.

Étude de cas 2 : le projet Liberty Alliance

Brève description du système

Créé en décembre 2001, le projet Liberty Alliance est un consortium regroupant actuellement plus de cent sociétés, associations sans but lucratif et gouvernements à travers le monde. Liberty Alliance n'a pas le statut de personne morale mais constitue un projet *ad hoc* auquel différentes sociétés participent, conformément aux termes d'un accord.

La mission du projet Liberty Alliance est d'élaborer des spécifications accessibles à tous en vue de développer un système d'identification fédéré sur l'internet. Les notions d'authentification simplifiée *(simplifiée! sign-on)* et d'identités fédérées *(federated network identity)* sont les piliers du système. Grâce à la signature unique *(single sign-on),* l'utilisateur s'identifie une seule fois auprès d'un fournisseur de services d'authentification et peut ensuite surfer sur les sites de plusieurs fournisseurs de services au sein d'un « cercle de confiance » *(trust domain),* sans devoir s'identifier à nouveau.

Le système fonctionnera au sein de « domaines ou cercles de confiance ». Il s'agit en fait d'une fédération de fournisseurs de services internet et de fournisseurs de services d'authentification qui sont commercialement liés entre eux, à travers la plate-forme Liberty Alliance, ou par des accords opérationnels, et avec lesquels des sociétés partenaires peuvent commercer au sein d'un environnement sécurisé et apparemment transparent.

Les spécifications du projet Liberty Alliance en sont encore à un stade de développement peu avancé et aucun système opérationnel n'est pour ainsi dire disponible pour l'instant[1]. Dans le futur, les spécifications du projet Liberty Alliance devraient semble-t-il être mises en œuvre par des entreprises du secteur des technologies de l'information et de la communication afin de mettre au point des systèmes compatibles avec la norme Liberty.

Analyse de la situation actuelle

— Tel qu'il se présente actuellement, le protocole permet de respecter les obligations de la directive. Le groupe de travail tient à insister sur le fait que Liberty Alliance est responsable du développement technique du projet. Le consortium Liber ty Alliance doit donc veiller à ce que les spécifications et le protocole qu'il met au point permettent à ceux qui les utilisent de respecter les dispositions de la directive. En outre, chacune des sociétés participantes est assimilée à un responsable du traite ment dès lors qu'elle exploite un site Liberty et aura donc la responsabilité de satis faire à la législation en vigueur en matière de protection des données.

— Le protocole Liberty Alliance est neutre au regard de la protection des don nées. Il permet de respecter la directive mais ne pousse en aucun cas à cela ; de plus, aucune mesure n'est prise en vue de faire respecter la mise en conformité. Le groupe de travail tient à encourager le consortium Liberty Alliance à formuler des recommanda tions et des lignes directrices destinées à motiver les sociétés afin qu'elles utilisent les spécifications tout en respectant, voire en renforçant, les principes de protection de la vie privée. Le système pourrait également intégrer certaines caractéristiques liées à la spécificité de la législation européenne dans ce domaine. Ce qui pourrait s'avérer par ticulièrement important pour les fournisseurs de services d'authentification se retrou vant à la tête d'une énorme quantité d'informations relatives aux utilisateurs.

— Le groupe de travail a constaté que bon nombre des sociétés associées au projet Liberty Alliance étaient implantées aux États-Unis ; aussi peut-on s'attendre à ce que l'utilisation des spécifications se traduise en pratique par le transfert d'un impor tant volume de données personnelles d'Europe vers les Etats-Unis. Le groupe de travail encourage les entreprises américaines partenaires du projet Liberty Alliance à garantir un niveau de protection adéquat aux données personnel es qui leur sont transférées.

— Actuellement, vu le développement très limité de Liberty Alliance et le fait que ce système ne soit pas encore opérationnel, il est difficile d'anticiper précisément quelles seront les conséquences du recours à un système reposant sur l'association de

[1] Sun One est compatible avec Liberty.

deux identités *(« pair-wised entities »).* Le groupe de travail souhaite cependant souligner que le système des codes d'identification associés présente l'avantage de ne pas créer d'identifiant unique pour l'utilisateur ; cependant il est nécessaire de continuer à examiner ces questions au regard de la protection des données personnelles, en particulier en ce qui concerne les possibilités techniques pour les sites de communiquer entre eux des données personnelles de l'utilisateur sans son consentement.

Bien que l'utilisation d'identités associées ait l'avantage de constituer un identifiant plus souple qu'un identifiant unique, la possibilité technique de communiquer ces différentes identités entre les sites participants reste une question délicate.

Quelques considérations sur les éventuels problèmes à l'avenir

Pour l'heure, les spécifications du projet Liberty Alliance ne constituent qu'un prototype qui n'a pour ainsi dire jamais été testé dans la pratique et qui, de toute évidence, fera l'objet de nombreuses modifications dans le futur.

Le groupe de travail tient dès lors à suivre le développement de ce système afin de garantir la prise en compte des obligations de la directive. Ainsi, il convient de considérer, par exemple, l'utilisation de « cookies », la possibilité pour les utilisateurs de réactualiser la valeur de l'identifiant numérique *(handle),* la fédération automatique, le rôle des fournisseurs de services d'authentification, la notion et le fonctionnement des « cercles de confiance » et les contrats qui seront conclus entre les sociétés utilisant une identité fédérée.

Le groupe de travail invite le consortium Liberty Alliance à réfléchir aux problèmes soulevés dans l'étude de cas n° 1 et à tenir compte des conclusions du dialogue avec Microsoft lors de l'examen de problèmes similaires à propos des spécifications du système. Plus particulièrement, l'utilisation d'identifiants dont la valeur numérique n'est pas librement accessible et d'identités associées, dans le contexte du projet Liberty Alliance, devrait être étudiée à la lumière des remarques formulées à propos du PUID.

Comparaison des systèmes d'authentification en ligne existants

Gestionnaire de mots de passe Mozilla	**Authentification via serveur proxy**	**Microsoft Passport**	**Liberty Alliance**
Pas de **tiers** fournisseur de services d'authentification	Tiers fournisseur de services d'authentification choisi par l'utilisateur final	Microsoft = tiers fournisseur de services d'authentification	Tiers fournisseur de services d'authentification choisi par le fournisseur de services (contrats mutuels)
Accès par PC propre uniquement	Accès *via* des canaux offerts par le fournisseur de services d'authentification	Accès possible *via* différents systèmes, à l'heure actuelle essentiellement de type PC	Accès possible n'a différents systèmes, dont téléphones mobiles
Actuellement disponible et largement utilisé	Disponibilité limitée	Actuellement disponible et utilisé par tous les services Microsoft	Premières phases de mise en œuvre
Nom d'utilisateur et mot de passe par site	Nom d'utilisateur et mot de passe par site	Nom d'utilisateur et mot de passe uniques	Nom d'utilisateur et mot de passe par site
Utilisateur identifié par nom d'utilisateur et mot de passe	Utilisateur identifié par nom d'utilisateur et mot de passe	Identifiant unique par utilisateur (PUID)	Valeur de l'identifiant numérique différente par sites associés

Gestionnaire de mots de passe Mozilla	Authentification via serveur proxy	Microsoft Passport	Liberty Alliance
Pas de contrat nécessaire	Contrat entre utilisateur et fournisseur	Contrat entre Microsoft et fournisseur de services	Contrat entre tous les sites au sein d'un cercle de confiance
	Protocole d'authentification exige du fournisseur de services proxy qu'il sache quels sites sont visités avec authentification (stockage de la combinaison UID/mof de passe par site)	Microsoft utilise un identifiant unique (PUID) par utilisateur	Valeur de l'identifiant numérique unique par paire de sites associés. Le fournisseur de services d'authentification doit connaître uniquement les sites où l'identité est fédérée
Du fait de la possibilité de multiplier les noms d'utilisateur, l'utilisateur final peut empêcher les fournisseurs de services de regrouper les données	Du fait de la possibilité de multiplier les noms d'utilisateur, l'utilisateur final peut empêcher les fournisseurs de services de regrouper les données	PUID unique identifie l'utilisateur. Accords contractuels empêchent les fournisseurs de services de regrouper leurs données	Regroupement des données utilisateurs uniquement possible par sites associés. Les sites déterminent leurs propres contrats mutuels
Fournisseur de services = seul responsable du traitement	Fournisseur de services et fournisseur de services proxy = responsables du traitement	Fournisseur de services traitant les demandes d'authentification et Microsoft sont responsables du traitement	Les fournisseurs de services au sein d'un cercle de confiance deviennent responsables du traitement quand les utilisateurs visitent leurs sites
Pas de transfert de données entre responsables du traitement	Données d'authentification transmises entre responsables du traitement	Données d'authentification et, dans certains cas, du profil transmis entre responsables du traitement	Données d'authentification transmises entre responsables du traitement
L'utilisateur contrôle toutes les communications	Consentement de l'utilisateur requis	Consentement de l'utilisateur requis (mise en œuvre par MS et par contrats)	En principe, consentement de l'utilisateur requis deux fois par fédération, mais fédération automatique possible
Protocole d'authentification ne requiert pas de « cookies »	Protocole d'authentification ne requiert pas de « cookies »	Configuration actuelle utilise des « cookies »	Configuration actuelle utilise des « cookies »

Conclusion

Le groupe de travail tient à insister sur le fait que les conclusions des deux études de cas doivent être considérées comme généralement applicables à tout système d'authentification en ligne, en présence d'applications soulevant des problèmes similaires. Les deux études de cas ont été choisies en fonction du développement actuel du marché des services d'authentification en ligne ; ceci dit, tous services similaires devraient tenir compte des mêmes considérations en matière de protection des données, lesquelles peuvent être résumées comme suit :

— Les concepteurs des systèmes d'authentification en ligne et ceux qui les mettent concrètement en œuvre (les fournisseurs de services d'authentification) sont responsables des aspects liés à la protection des données, mais à des degrés différents. Les sites web qui utilisent ces systèmes (les fournisseurs de services) ont également leur propre responsabilité au sein du processus. Il est conseillé aux différentes parties prenantes de conclure entre elles des accords contractuels dans lesquels sont exposées de manière explicite les obligations de chacune des parties.

— Dans la mesure du possible, il convient de tout mettre en œuvre pour faciliter l'utilisation des services d'authentification en ligne sous couvert d'anonymat ou

sous un pseudonyme. Dans les cas où l'application de cette règle entrave le bon fonctionnement du système, celui-ci devrait être conçu de manière à exiger un minimum d'informations aux fins d'authentification de l'utilisateur et à permettre à ce dernier d'avoir un contrôle total sur la décision concernant quelles informations supplémentaires fournir (telles que les données relatives à son profil). Cette liberté de décision doit être offerte tant par le fournisseur de services d'authentification que par les fournisseurs de services (les sites qui utilisent le système).

— Il est capital de fournir une information adéquate aux utilisateurs sur les implications du système au regard de la protection des données (identité du respon sable du traitement, finalité du traitement, données collectées, destinataires, etc.). Cette information doit être facilement accessible et présentée de manière conviviale, de préférence par un formulaire en ligne de collecte de données ou par un *« pop up »* qui s'ouvrirait sur l'écran de l'utilisateur, et ce dans toutes les langues dans les quelles le service est offert.

— Lorsque des données personnelles doivent être transférées vers des pays tiers, les fournisseurs de services d'authentification devraient travailler avec des four nisseurs de services qui prennent toutes les mesures nécessaires pour assurer un niveau de protection adéquat[1] ou qui offrent des garanties suffisantes eu égard à la protection des données personnelles des utilisateurs du système. Ces garanties peu vent être offertes par le biais de la conclusion de contrats ou de l'application de règles d'entreprise contraignantes. Cette solution devrait être la règle générale.

— Si, dans des cas particuliers uniquement, le transfert repose sur le consen tement de l'utilisateur, celui-ci doit être suffisamment informé et doit être libre d'accepter ou de refuser le transfert, au cas par cas.

— L'utilisation d'identifiants, quelle que soit leur forme, suppose des risques pour la protection des données. Il convient d'étudier toutes les alternatives possibles. Si le recours à des identifiants s'avère indispensable, la possibilité de permettre à l'utilisateur de réactualiser ces identifiants devrait être envisagée.

— L'adoption d'une architecture logicielle minimisant la centralisation des données personnelles des utilisateurs internet serait appréciable et est encouragée, dans la mesure où elle améliorerait les propriétés de tolérance des erreurs du système d'authentification *(faulf-tolerance propertiesj,* et éviterait la création de bases de données à valeur ajoutée détenue, et gérée, par une société unique ou par un petit groupe de sociétés ou d'organisations.

— Les utilisateurs peuvent facilement exercer leurs droits (y compris leur droit d'opposition *(opt-out))* et effacer l'ensemble de leurs données s'ils décident de ne plus utiliser un système donné d'authentification en ligne. Ceux-ci devraient être correctement informés de la procédure à suivre pour poser des questions ou intro duire une plainte.

— Dans ce contexte, la sécurité joue un rôle capital. Des mesures d'ordre organisationnel et technique, adaptées aux risques potentiels, devraient être prises.

En raison de la nature évolutive du service .NET Passport, du projet Liberty Alliance ainsi que d'autres services d'authentification similaires, le groupe de travail continuera à suivre les développements ultérieurs dans ce domaine, en particulier en s'assurant de ce que les engagements pris par Microsoft seront respectés dans le cadre de l'échéancier prévu, tel que détaillé au paragraphe *supra.*

[1] Ce cas peut s'appliquer notamment aux sociétés américaines admissibles à la sphère de sécurité, lesquelles devraient être encouragées à y adhérer. Ceci ne s'applique évidemment pas aux cas dans lesquels la société établie dans un pays tiers ne relève pas du champ d'application de la directive.

Annexe 8

Décisions des juridictions

ARRÊT DU CONSEIL D'ÉTAT DU 3 JUILLET 2002
(Req. n° 157402)

Vu le recours du ministre de l'Équipement, des Transports et du Tourisme, enregistré le 29 mars 1994 au secrétariat du contentieux du Conseil d'Etat ; le ministre demande au Conseil d'État :
1) d'annuler le jugement du 13 juillet 1993 par lequel le tribunal administratif de Strasbourg a annulé, à la demande de M. X..., président de l'Association française de l'apprentissage de la conduite, le refus implicite du préfet de la Moselle de lui communiquer les statistiques de réussite au permis de conduire établies par auto-école dans son département ;
2) de rejeter la demande présentée par le président de l'Association française de l'apprentissage de la conduite devant le tribunal administratif de Strasbourg ;

Vu les autres pièces du dossier ; Vu la

loi n° 78-17 du 6 janvier 1978 ;

Vu la loi n° 78-753 du 17 juillet 1978 modifiée par la loi n° 79-587 du 11 juillet 1979 ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :
— le rapport de M. Ménéménis, maître des requêtes ;
— les conclusions de M. Courtial, commissaire du gouvernement ;

Considérant que l'Association française de l'apprentissage de la conduite (AFAC) a demandé au préfet de la Moselle, sur le fondement de la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, communication de statistiques récapitulant, pour chacune des auto-écoles du département de la Moselle, d'une part le nombre d'élèves présentés et reçus à l'examen du permis de conduire, d'autre part le taux de réussite à cet examen calculé sur la base de ces éléments ; qu'à la suite du refus opposé par le préfet à cette demande, l'AFAC a saisi la Commission d'accès aux documents administratifs qui a émis, le 27 mai 1992, un avis favorable à la communication de ces documents, sous réserve de l'occultation des mentions relatives aux effectifs des candidats présentés, au motif que la communication de cet élément serait de nature à porter atteinte au secret en matière commerciale et industrielle au sens de l'article 6 de la loi du 17 juillet 1978 ; que le préfet n'a pas donné suite à la nouvelle demande formulée par l'AFAC à la suite de cet avis ; que l'AFAC a formé devant le tribunal administratif de Strasbourg un recours en annulation de la décision de rejet née du silence gardé par le préfet ; que le ministre de l'Équipement, des Transports et du Tourisme fait appel du jugement par lequel le tribunal administratif a annulé le refus implicite du préfet ;

Considérant qu'aux termes de l'article 4 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa rédaction alors applicable : *« Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification de personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale »* ; qu'aux termes de l'article 5 de ladite loi : *« Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par des moyens informatiques, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conser-*

vation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives » ; qu'il résulte des termes de ces dispositions législatives, éclairées au surplus par leurs travaux préparatoires, que les informations nominatives qu'elles mentionnent sont celles qui permettent d'identifier des personnes physiques ; que les entrepreneurs individuels, pris en cette qualité, ne sont pas des personnes physiques pour l'application de ces dispositions ;

Considérant qu'il ressort des pièces du dossier que, si les statistiques dont l'AFAC demande communication sont issues d'un traitement automatisé d'informations, elles ne contiennent aucune donnée permettant l'identification de personnes physiques, ni aucun élément constituant une information nominative, au sens des dispositions susanalysées de la loi du 6 janvier 1978 ; qu'ainsi, le ministre n'est pas fondé à soutenir que le tribunal administratif aurait commis une erreur de droit en jugeant que la communication des statistiques en cause était régie par les dispositions précitées de la loi du 17 juillet 1978 et non par celles de la loi du 6 janvier 1978 ;

Considérant qu'aux termes de l'article 1er de la loi du 17 juillet 1978 modifiée portant mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal dans sa rédaction alors applicable : *« Le droit de toute personne à l'information est garanti par le présent titre, en ce qui concerne la liberté d'accès aux documents administratifs de caractère non nominatif. Sont considérés comme documents administratifs au sens du présent titre tous dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires* [...] *prévisions et décisions revêtant la forme d'écrits, d'enregistrements sonores et visuels, de traitements automatisés d'informations non nominatives »* ; qu'aux termes de l'article 2 de cette loi : *« Sous réserve des dispositions de l'article 6, les documents administratifs sont de plein droit* communi*cables aux personnes qui en font la demande »* ; qu'aux termes de l'article 6 de ladite loi : « *Les administrations* [...] *peuvent refuser de laisser consulter ou de communiquer un document dont la consultation ou la communication porterait atteinte […]. au secret en matière commerciale et industrielle […] »* ; qu'aux termes de l'article 6 bis de cette loi : *« Les personnes qui le demandent ont droit à la communication [...] des documents de caractère nominatif les concernant [...] »* ; qu'au sens de ces dispositions, éclairées notamment par les travaux préparatoires de la loi du 17 juillet 1978, revêtent un caractère nominatif les documents qui permettent de porter une appréciation ou un jugement de valeur sur une personne physique nommément désignée ou facilement identifiable ;

Considérant qu'il ressort des pièces du dossier que les statistiques demandées par l'AFAC, qui récapitulent le nombre de candidats présentés à l'examen du permis de conduire et le taux de réussite à cet examen des différentes auto-écoles, ne contiennent aucun élément de caractère nominatif au sens des dispositions de la loi du 17 juillet 1978 ; qu'elles ne comportent par ailleurs aucune indication relevant du secret en matière commerciale et industrielle au sens de l'article 6 de cette loi ; que, par suite, le ministre n'est pas fondé à soutenir que les statistiques en cause n'auraient pas le caractère de documents administratifs communicables au sens de la loi du 17 juillet 1978 ;

Considérant qu'il résulte de ce qui précède que le ministre n'est pas fondé à soutenir que c'est à tort que le tribunal administratif de Strasbourg a annulé le refus implicite au préfet de la Moselle de communiquer à l'AFAC les statistiques retraçant

le taux de réussite à l'examen du permis de conduire de chaque auto-école du département de la Moselle ;

Décide :

Article 1er : le recours du ministre de l'Equipement, des Transports et du Tourisme est rejeté.

Article 2 : la présente décision sera notifiée au ministre de l'Équipement, des Transports et du Tourisme et de la Mer et à l'Association française de l'apprentissage de la conduite.

ARRÊT DU CONSEIL D'ÉTAT DU 6 NOVEMBRE 2002 (Req. n° 194296)

Vu 1°), sous le n° 194296, la requête, enregistrée au secrétariat du contentieux du Conseil d'État le 18 février 1998, présentée pour Mme X..., ; Mme X... demande que le Conseil d'État :
1) annule la décision en date du 29 septembre 1997 de la Commission nationale de l'informatique et des libertés prise sur sa demande tendant d'une part, à ce que lui soient communiquées les informations la concernant figurant dans le système informatique national du système d'information Schengen et d'autre part, à ce que ces données soient rectifiées ou effacées ;
2) condamne l'État à lui verser la somme de 20 000 F sur le fondement de l'article 75-1 de la loi du 10 juillet 1991 ;

Vu 2°), sous le n° 219588, enregistrée au secrétariat du contentieux du Conseil d'État le 31 mars 2000, l'ordonnance en date du 27 mars 2000 par laquelle le président du tribunal administratif de Paris transmet au Conseil d'État, en application des dispositions de l'article R. 67 du Code des tribunaux administratifs et des cours administratives d'appel le dossier de la requête dont ce tribunal a été saisi par Mme X... ;

Vu la demande présentée le 25 juin 1998 au greffe du tribunal administratif de Paris par Mme X... ; Mme X... demande :
1) d'annuler la décision implicite de rejet résultant du silence gardé par le ministre de l'Intérieur sur sa demande tendant à l'effacement des données la concernant et enregistrées dans le système d'information Schengen ;
2) d'enjoindre au ministre de l'Intérieur de procéder à l'effacement des données la concernant et contenues dans le système d'information Schengen ;
3) de condamner l'État à lui verser la somme de 25 000 F au titre de l'article L. 8-1 du Code des tribunaux administratifs et des cours administratives d'appel ;

Vu les autres pièces des dossiers ;

Vu la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales ;

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

Vu la loi n° 80-539 du 16 juillet 1980, notamment son article 6-1 ;

Vu la loi n° 91-737 du 30 juillet 1991 autorisant l'approbation de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique du Bénélux, de la République fédérale d'Allemagne, de la République française relative à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 ;

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

Vu le décret n° 79-1160 du 28 décembre 1979 ;

Vu le décret n° 86-326 du 7 mars 1986 ;

Vu le décret n° 95-304 du 21 mars 1995 portant publication de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique du Bénélux, de la République fédérale d'Allemagne, de la République française relative à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 ;

Vu le décret n° *95-577* du 6 mai 1995 relatif au système informatique national du système d'information Schengen dénommé N-SIS ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :

— le rapport de M. Mochon, maître des requêtes ;
— les observations de la SCP Delaporte, Briard, avocat de M^me^ X... ;
— les conclusions de M^me^ Maugüé, Commissaire du gouvernement ;

Considérant que M^me^ X... s'est vu opposer le 11 novembre 1995, alors qu'elle était en transit à l'aéroport Roissy — Charles de Gaulle, une décision lui interdisant de poursuivre un voyage à destination de l'Espagne au motif qu'elle faisait l'objet d'un signalement *aux* fins de non admission dans le fichier du système d'information Schengen ; qu'elle a, en premier lieu, saisi la Commission nationale de l'informatique et des libertés (CNIL) en lui demandant la communication et, le cas échéant, la rectification ou l'effacement des informations figurant à son sujet dans ce fichier ; que, par la requête n° 194296, elle demande l'annulation de la décision du 29 septembre 1997 par laquelle la CNIL s'est bornée à l'informer qu'il avait été procédé aux vérifications prévues par les dispositions de l'article 39 de la loi du 6 janvier 1978 ; que M^me^ X... a, en deuxième lieu, demandé au ministre de l'Intérieur par lettre du 26 août 1997 l'effacement des informations figurant à son sujet dans le même fichier ; que, par la requête n° 219588, elle demande l'annulation de la décision implicite de rejet de cette demande ;

Considérant que le Conseil d'État est compétent pour connaître en premier ressort de la requête n° 194296 de M^me^ X... dirigée contre la décision par laquelle la Commission nationale de l'informatique et des libertés, en se bornant à l'informer de ce qu'il avait été procédé aux vérifications prévues par l'article 39 de la loi du 6 janvier 1978, a rejeté le surplus de sa demande ;

Considérant qu'il y a lieu de statuer par une seule décision sur les requêtes n° 194296 et n° 219588, qui émanent d'un même demandeur et présentent à juger des questions semblables ;

Considérant, d'une part, que l'article 92 de la convention d'application de l'accord de Schengen du 14 juin 1985 institue un « système d'information Schengen » composé d'une partie nationale auprès de chacune des parties contractantes et d'une fonction de support technique ; que ce système a pour objet, conformément à l'article 93 de ladite convention, *« de préserver l'ordre et la sécurité publics y compris la sûreté de l'État, et l'application des dispositions sur la circulation des personnes de la présente convention, sur les territoires des parties contractantes à l'aide des informations transmises par ce système »* ; qu'aux termes de l'article 106 de la convention d'application de l'accord de Schengen : « 7. *Seule la partie contractante signalante est autorisée à modifier, à compléter, à rectifier ou à effacer les données qu'elle* a *introduites. /2. Si une des parties contractantes qui n'a pas fait le signale-*

ment dispose d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, elle en avise dans les meilleurs délais la partie contractante signalante qui doit obligatoirement vérifier la communication, et si nécessaire, corriger ou effacer la donnée sans délai. […] » ; que le droit d'accès au système d'information Schengen est régi par l'article 109 de la convention, qui stipule : « *Le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le système d'information Schengen s'exerce dans le respect du droit de la partie contractante auprès de laquelle elle le fait valoir. Si le droit national le prévoit, l'autorité nationale de contrôle prévue à l'article 714 paragraphe* 1 *décide si des informations sont communiquées et selon quelles modalités »* ; que l'article 110 de la même convention stipule : *« Toute personne peut faire rectifier des données entachées d'erreur de fait la concernant ou faire effacer des données entachées d'erreur de droit la concernant »* ; qu'aux termes de l'article 111 de la convention : *« 1. Toute personne peut saisir, sur le territoire de chaque partie* contractante, *la juridiction ou l'autorité compétentes en vertu du droit national, d'une action notamment en rectification, en effacement, en information ou en indemnisation en raison d'un signalement la concernant, (à) »* ; qu'enfin, l'article 114 stipule : « 1. *Chaque partie contractante désigne une autorité de contrôle chargée, dans le respect du droit national, d'exercer un contrôle indépendant du fichier de la partie nationale du système d'information Schengen et de vérifier que le traitement et l'utilisation des données intégrées dans le système d'information Schengen ne sont pas attentatoires aux droits de la personne concernée* [...] *2. Toute personne a le droit de demander aux autorités de contrôle de vérifier les données la concernant intégrées dans le système d'information Schengen ainsi que l'utilisation qui est faite de ces données. Ce droit est régi par le droit national de la partie contractante auprès de laquelle la demande est introduite […]* » ;

Considérant qu'en application des stipulations précitées de l'article 106 de la convention d'application de l'accord de Schengen, il incombe aux autorités nationales, saisies par une personne qui conteste son inscription dans le système informatique national du système d'information Schengen, de procéder, dans le cas d'un signalement opéré par la France, à l'effacement des données entachées d'erreur de droit ou d'erreur de fait ; que, dans le cas d'un signalement opéré par un État autre que la France, il appartient aux autorités nationales, si elles estiment disposer d'indices faisant présumer qu'une donnée est entachée d'erreur de droit ou de fait, d'en aviser les autorités de cet Etat ;

Considérant, d'autre part, qu'aux termes de l'article 36 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *Le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant et qui sont inexactes, incomplètes,* équivoques, *périmées ou dont la collecte et l'utilisation, la communication ou la conservation est interdite »* ;

Considérant qu'aux termes de l'article 39 de la loi du 6 janvier 1978 : *« En ce qui concerne les traitements intéressant la sûreté de l'Etat, 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'Etat, à la Cour de Cassation ou à la Cour des comptes pour mener foutes investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la Commission. Il est notifié au requérant qu'il a été procédé aux vérifications »* ; que, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, il peut comprendre, d'une part, des informations dont la communication à l'intéressé serait susceptible de mettre en cause les fins assignées à ce traitement et, d'autre part, des

informations dont la communication ne mettrait pas en cause ces mêmes fins, et notamment des décisions administratives ou juridictionnelles qui ont été ou auraient dû préalablement être communiquées à l'intéressé ; que, pour les premières, il incombe à la Commission nationale de l'informatique et des libertés, saisie par la personne visée par ces informations, de l'informer qu'il a été procédé aux vérifications nécessaires ; que, pour les autres, il appartient au gestionnaire du traitement ou à la Commission nationale de l'informatique et des libertés, saisis par cette personne, de lui en donner communication, avec, pour la Commission, l'accord du gestionnaire du traitement ;

Considérant qu'aux termes de l'article 6 du décret du 6 mai 1995 relatif au système informatique national du système d'information Schengen, le droit d'accès aux données enregistrées dans ce système informatique *« s'exerce auprès de la Commission nationale de l'informatique et des libertés, conformément aux articles 109 et 114 de la convention et à l'article 39 de la loi du 6 janvier 7 978 susvisée sans préjudice des dispositions réglementaires relatives aux données susceptibles d'être consultées directement par l'intéressé exerçant ce droit. »*

Sur les conclusions de M^me^ X... tendant à l'annulation de la décision de la Commission nationale de l'informatique et des libertés du 29 septembre 1997 :

En ce qui concerne le moyen excipant de l'illégalité du décret du 6 mai 1995 :

Considérant que M^me^ X... excipe de l'illégalité des dispositions de l'article 6 du décret du 6 mai 1995 en soutenant, en premier lieu, que celui-ci serait contraire aux stipulations de la convention d'application de l'accord de Schengen et, en second lieu, qu'il méconnaîtrait l'article 39 de la loi du 6 janvier 1978 en tant qu'il n'autoriserait pas la Commission nationale de l'informatique et des libertés à donner à l'intéressé accès à certaines des informations le concernant et figurant dans le système national du système d'information Schengen ;

Considérant qu'il résulte des stipulations des articles 109 et 114 de la convention d'application de l'accord de Schengen que le droit d'accès au fichier du système d'information Schengen s'exerce dans le cadre du droit national du pays clans lequel la demande est présentée ; qu'en tant qu'il prévoit que les informations contenues dans le système d'information Schengen font l'objet d'un droit d'accès dans les conditions de l'article 39 de la loi du 6 janvier 1978, le décret est compatible avec l'article 109 de la convention, qui renvoie au droit national pour déterminer en particulier si l'autorité nationale de contrôle, qui est en France la Commission nationale de l'informatique et des libertés, peut décider que des informations sont communiquées et selon quelles modalités ; que le décret est également compatible avec les droits de rectification et d'effacement énoncés à l'article 110 ; qu'il est conforme aux dispositions de l'article 39 de la loi du 6 janvier 1978 auquel son article 6 renvoie expressément pour la définition des modalités du droit d'accès ;

En ce qui concerne les autres moyens :

Considérant que M^me^ X..., pour demander l'annulation de la décision de la Commission nationale de l'informatique et des libertés en tant qu'elle lui refuse l'accès aux informations la concernant qui seraient intégrées dans le système informatique national du système d'information Schengen et en tant qu'elle refuserait de faire procéder à la rectification de ces informations, soutient que ces informations devaient lui être communiquées sur le fondement de l'article 39 de la loi du 6 janvier 1978 et qu'elles devaient être rectifiées ou effacées ;

Considérant que, parmi les informations relatives à M^me^ X... et susceptibles de figurer dans le système informatique national du système d'information Schengen,

certaines pourraient devoir lui être communiquées tandis que d'autres, qui mettent en cause les fins du traitement, ne seraient pas susceptibles de l'être ; que, cependant, l'état de l'instruction ne permet de déterminer, ni si les informations concernant M^me^ X... et figurant dans ce fichier devaient lui être communiquées, ni si la Commission nationale de l'informatique et des libertés a fait procéder, le cas échéant, à la rectification ou à l'effacement de ces informations ;

Considérant que si, conformément au principe du caractère contradictoire de l'instruction, le juge administratif est tenu de ne statuer qu'au vu des seules pièces du dossier qui ont été communiquées aux parties, il lui appartient, dans l'exercice de ses pouvoirs généraux de direction de la procédure, de prendre toutes mesures propres à lui procurer, par les voies de droit, les éléments de nature à lui permettre de former sa conviction sur les points en litige ;

Considérant qu'en l'espèce, il y a lieu pour le Conseil d'État d'ordonner à la Commission nationale de l'informatique et des libertés de lui communiquer — pour versement au dossier de l'instruction écrite contradictoire — tous éléments utiles à la solution du litige et relatifs aux informations concernant l'inscription, à la date de sa décision du 29 septembre 1997, de M^me^ X... dans le système informatique national du système d'information Schengen ainsi qu'aux vérifications auxquelles la Commission s'est livrée en réponse à la demande présentée par M^me^ X... en application des dispositions de l'article 39 de la loi du 6 janvier 1978 ; que, dans l'hypothèse où la Commission nationale de l'informatique et des libertés estimerait que ces informations, ou certaines d'entre elles, sont couvertes par un secret garanti par la loi ou que, s'agissant de données intéressant la sûreté de l'État, la défense et la sécurité publique, leur communication mettrait en cause les fins assignées à ce fichier, et où elle estimerait en conséquence devoir refuser leur communication, il lui appartiendrait néanmoins de verser au dossier de l'instruction écrite contradictoire tous éléments d'information appropriés sur la nature des pièces écartées et les raisons de leur exclusion, de façon à permettre au Conseil d'Etat de se prononcer en connaissance de cause sans porter, directement ou indirectement, atteinte aux secrets garantis par la loi ou imposés par des considérations tenant à la sûreté de l'Etat, à la défense et à la sécurité publique ; qu'enfin, dans le cas où un refus serait opposé à une demande d'information formulée par lui, il appartiendrait au Conseil d'État, conformément aux règles générales d'établissement des faits devant le juge administratif, de joindre, en vue du jugement à rendre, cet élément de décision à l'ensemble des données fournies par le dossier ;

Sur les conclusions de M^me^ X... tendant à l'annulation de la décision implicite du ministre de l'Intérieur :

Considérant que la demande adressée par M^me^ X... au ministre de l'Intérieur tendait à obtenir l'effacement des données la concernant et figurant dans le système informatique national du système d'information Schengen ; qu'en rejetant implicitement la demande de M^me^ X..., le ministre a, dans l'hypothèse où un signalement aurait été opéré par la France, refusé de procéder à l'effacement des données et, dans l'hypothèse où un signalement aurait été opéré par un État autre que la France, refusé de saisir les autorités de cet État ;

Considérant que l'état de l'instruction ne permet ni de connaître l'ensemble des motifs de l'inscription de M^me^ X... dans le système informatique national du système d'information Schengen ni, par conséquent, d'apprécier fa légalité du refus opposé par le ministre à la demande d'effacement dont celui-ci était saisi ni de contrôler la mise en œuvre des mesures d'effacement ou de correction éventuellement ordonnées par la Commission nationale de l'informatique et des libertés ; qu'il y a

donc lieu, dans les mêmes conditions que celles mentionnées ci-dessus, d'ordonner avant-dire-droit au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales de communiquer au Conseil d'État tous éléments utiles à la solution du litige et relatifs aux informations concernant l'inscription de M^me^ X... dans le système informatique national du système d'information Schengen à la date de la décision attaquée ;

Décide :

Article 1^er^ : avant-dire-droit sur les requêtes n° 194296 et n° 219588 de M^me^ X..., tous droits et moyens des parties demeurant réservés, à l'exception de ceux sur lesquels il est statué par la présente décision, il est ordonné à la Commission nationale de l'informatique et des libertés, d'une part, au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, d'autre part, de communiquer au Conseil d'Etat, dans un délai de deux mois, les informations définies par les motifs de la présente décision.

Article 2 : la présente décision sera notifiée à M^me^ X..., au président de la Commission nationale de l'informatique et des libertés et au ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales.

ARRÊT DU CONSEIL D'ÉTAT DU 13 DÉCEMBRE 2002 (Req. n° 237976)

Vu la requête, enregistrée le 6 septembre 2001 au secrétariat du contentieux du Conseil d'État, présentée par M. X..., ; M. X... demande au Conseil d'État :
1) d'ordonner avant-dire-droit la communication des données le concernant figurant au, fichier du Conseil d'État, de l'avis rendu par la section de l'intérieur du Conseil d'État préalablement à la signature du décret attaqué, et des conclusions du commis saire au gouvernement ;
2) d'annuler le décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dis positions du troisième alinéa de l'article 31 de la loi n° 78-17 du 6 janvier 1978 rela tive à l'informatique, aux fichiers et aux libertés et portant création d'un système de traitement des infractions constatées ;

Vu les autres pièces du dossier ;

Vu le Code de procédure pénale ;

Vu la loi n° 78-17 du 6 janvier 1978 ;

Vu le décret n° 78-774 du 17 juillet 1978 ;

Vu le décret n° 79-1160 du 28 décembre 1979 ;

Vu le décret n° 90-115 du 2 février 1990 ;

Vu le Code de justice administrative ;

Après avoir entendu en séance publique :
— le rapport de M. Wauquiez-Motte, auditeur ;
— les conclusions de M. Vallée, commissaire du gouvernement ;

En ce qui concerne les conclusions aux fins d'annulation du décret du 5 juillet 2001 pris pour l'application des dispositions du 3^e^ alinéa de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

Considérant que le décret attaqué autorise le ministère de l'Intérieur (Direction générale de la police nationale) à mettre en oeuvre une application automatisée d'informations nominatives dénommée « système de traitement des infractions constatées » (STIC), dont la finalité est l'exploitation des informations contenues dans les

procédures établies par les services de police, dans le cadre de leur mission de police judiciaire, aux fins de recherches criminelles et de statistiques ;

Sur la légalité externe

Considérant que le décret attaqué prévoit en son article 8 que le droit d'accès s'exerce d'une manière indirecte, dans les conditions prévues à l'article 39 de la loi du 6 janvier 1978, par demande portée devant la Commission nationale de l'informatique et des libertés ; que, toutefois, la Commission peut constater, en accord avec le ministère de l'Intérieur, que des informations nominatives enregistrées ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique et qu'il y a donc lieu de les communiquer à la personne intéressée, sous réserve que la procédure soit judiciairement close et après accord du procureur de la République ;

Considérant que cette procédure met en œuvre, s'agissant de l'application automatisée d'informations nominatives régie par le décret attaqué, les règles posées par l'article 39 de la loi du 6 janvier 1978 ; que le moyen tiré de ce que le pouvoir réglementaire aurait incompétemment institué une telle procédure doit donc être écarté ;

Sur la légalité interne

Considérant, d'une part, qu'aux termes de l'article 12 du Code de procédure pénale : *« La police judiciaire est exercée, sous la direction du procureur de la République, […] »* ; qu'aux termes de l'article 14 du même code, la police judiciaire est *« chargée […] de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs tant qu'une information n'est pas ouverte. Lorsqu'une information est ouverte, elle exécute les délégations des juges d'instruction et défère à leurs réquisitions »* ; qu'ainsi, la constatation des infractions est une mission confiée par le Code de procédure pénale à la police judiciaire et exercée sous le contrôle d'un magistrat ;

Considérant, d'autre part, que la collecte des données par les services de police judiciaire dans le cadre des missions qui leur sont imparties ne préjuge pas de la qualification éventuelle d'infractions qui sera déterminée par les magistrats de la juridiction compétente ; qu'en outre, l'article 3 du décret attaqué prévoit un contrôle du procureur de la République territorialement compétent pour le traitement des informations nominatives collectées et la possibilité offerte aux personnes concernées d'exiger que la qualification des faits finalement retenue par l'autorité judiciaire soit substituée à la qualification initialement mentionnée dans le fichier ; que le requérant n'est donc pas fondé à soutenir que le décret attaqué serait illégal en tant qu'il autorise l'enregistrement d'informations considérées comme relatives à des infractions constatées, avant que la juridiction compétente ne se soit prononcée ;

Considérant enfin que l'article 8 précité du décret attaqué ménage, dans les conditions susmentionnées, un droit d'accès aux données collectées dans le « Système de traitement des infractions constatées » ; que si, aux termes de l'article 9 du décret attaqué, le droit d'opposition prévu à l'article 26 de la loi du 6 janvier 1978 susvisée est inapplicable, les victimes d'infractions peuvent en revanche s'opposer à ce que les données nominatives les concernant soient conservées ; que les durées de conservation de l'ensemble des données ont été plafonnées dans les conditions fixées par l'article 7 du décret attaqué ; qu'enfin, l'article 3 prévoit que sont supprimées les informations relatives aux personnes ayant bénéficié de décisions de relaxe ou d'acquittement devenues définitives ; que le requérant n'est donc pas fondé à soutenir que, faute d'avoir prévu un accès aux données du « Système de traitement des

infractions constatées » et la possibilité d'en obtenir la modification, le décret attaqué serait contraire aux exigences de la loi du 6 janvier 1978 ;

Considérant qu'il résulte de ce qui précède que M. X... n'est pas fondé à demander l'annulation du décret du 5 juillet 2001 ;

En ce qui concerne les autres conclusions de la requête :

Considérant, d'une part, qu'il n'appartient pas, en tout état de cause, au Conseil d'État statuant au contentieux, en l'absence d'un recours contre une décision de rejet des demandes de communication de documents formulées par le requérant, d'ordonner cette communication ; que, d'autre part, les conclusions du commissaire du gouvernement ne sont pas des documents destinés à être préalablement communiqués aux parties ;

Décide :

Article 1er : la requête de M. X... est rejetée.

Article 2 : la présente décision sera notifiée à M. X..., au Premier ministre et au garde des Sceaux, ministre de la Justice.

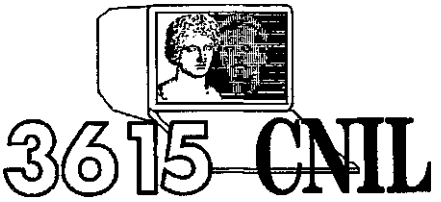
Table des matières

Commission nationale
de l'informatique et des libertés

21, rue Saint-Guillaume
75340 Paris Cedex 07

Tél. 01 53 73 22 22
Télécopie : 01 53 73 22 00

POUR PLUS D'INFORMATIONS :



Site Internet : http ://www.cnil.fr

Imprimé en France par INSTAPRINT S.A.
1-2-3, levée de la Loire - LA RICHE - B.P. 5927 - 37059 TOURS Cedex 1
Tél. 02 47 38 16 04

Dépôt légal 2e trimestre 2003

23e rapport d'activité 2002

Intense et multiforme, l'activité de la Commission nationale de l'informatique et des libertés, reflet des missions qui lui sont dévolues par la loi du 6 janvier 1978, est retracée en détail dans ce 23e rapport annuel.

Sept chapitres thématiques présentent dans une première partie les grands sujets traités par la CNIL en 2002, étayés d'exemples concrets issus des plaintes les plus significatives. Un éclairage international, en particulier celui de la coopération européenne, est systématiquement apporté.

La deuxième partie de ce rapport reprend l'intégralité des délibérations adoptées par la CNIL en 2002 et constitue un outil de travail précieux pour les juristes et les praticiens qui souhaiteraient accéder directement au texte de ses décisions.

Fichiers de police, *« spamming »,* vote électronique, refus de crédit ou d'abonnement téléphonique, anonymisation des décisions de justice, conservation du numéro de carte bancaire, accès au dossier médical, changement d'adresse, recensement... : autant de sujets au quotidien, autant d'enjeux pour la protection des données et la vie privée.

Prix : **22€**
La Documentation française
29-3 1, quai Voltaire
75344 Paris Cedex 07
Téléphone : 01 40 15 70 00
Télécopie : 01 40 1 5 72 30
www.ladocumentationfrancaise.fr
Imprimé en France
ISBN : 2-11-005434-4
DF : 5 7099-0

9 782110054340