Guy BRAIBANT

DONNEES PERSONNELLES ET SOCIETE DE L'INFORMATION

Rapport au Premier Ministre sur la transposition en droit français de la directive no 95/46

le 3 mars 1998

Introduction

LES ENJEUX

Les progrès intervenus dans le domaine informatique depuis vingt ans ont bouleversé les enjeux de la protection des données à caractère personnel. Pour percevoir l'intensité de ces progrès et des bouleversements qui en découlent, il suffit de réaliser que, pendant cette période, les progrès scientifiques et technologiques ont permis de multiplier par mille la vitesse de traitement de l'information, les capacités de stockage et les capacités de communication.

Les années 1970 ont vu le développement des systèmes macro-informatiques dans les grandes organisations, notamment les administrations publiques. L'ordinateur individuel n'est né qu'à la fin de la décennie (le premier IBM PC a été mis sur le marché en 1981). L'informatique restait essentiellement une affaire de spécialistes, mal connue et peu diffusée dans le grand public.

L'ordinateur était perçu comme un instrument de renforcement de l'efficacité des organisations publiques dans leurs relations avec les administrés, notamment pour l'exercice de leurs fonctions de contrôle, dans les matières fiscale et policière. Les consciences – en France comme dans d'autres pays européens – étaient marquées par les représentations les plus sombres d'une administration appelée à investir progressivement la sphère privée : le retentissant article de Philippe Boucher paru dans *Le Monde* en 1974, " SAFARI ou la chasse aux Français ", faisait écho à *1984* de George Orwell.

Les mesures législatives adoptées dans ce contexte par plusieurs pays occidentaux, dont la France, avaient donc pour objet premier de protéger le citoyen contre les dérives policières auxquelles la mise en œuvre de traitements centralisés et l'exploitation systématique de données personnelles pouvaient conduire les principales administrations publiques. Les enjeux et les risques liés au développement de l'informatique d'entreprise étaient peu ou mal appréhendés par l'opinion.

Ces données de base ont été profondément modifiées par le développement de la micro-informatique, par sa très large diffusion dans les entreprises et auprès des particuliers, et enfin par l'intégration croissante des outils informatiques en réseaux.

Le citoyen passif, mis en fiches par les grandes organisations, est devenu un utilisateur actif des moyens informatiques, depuis la carte de crédit jusqu'au poste multimédia, personnel ou professionnel.

L'informatique s'est banalisée au point de devenir indispensable à l'essentiel des activités courantes, en même temps que les risques induits par son utilisation se sont démultipliés.

Les bases de données sont désormais transférables en un instant d'un point à l'autre du globe, par téléchargement. De puissants moteurs de recherche permettent d'opérer des croisements et des synthèses de fichiers sans avoir recours à une nomenclature commune.

Les moyens d'interconnexion et de traitement de masse existaient à la fin des années 1970, mais leur coût était tel que seule une administration ou une entreprise multinationale pouvait les

mettre en œuvre. Ils sont désormais accessibles, pour un coût limité, à n'importe quel particulier ou opérateur privé équipé d'un micro-ordinateur connecté au réseau téléphonique.

Dans le même temps, la nature des données personnelles susceptibles d'être traitées s'est diversifiée à l'infini, englobant aussi bien la voix et l'image que les empreintes digitales ou le génome humain. La quantité d'informations recueillies sur chaque individu, le nombre de traitements dont elles sont susceptibles de faire l'objet, dépassent ce qu'il est susceptible d'appréhender.

LES BENEFICES DU PROGRES TECHNIQUE

Libre circulation des données et liberté d'information et d'expression

L'informatique d'entreprise : liberté d'entreprendre et libre circulation des données

Pour exercer leur mission et leur fonction sociale, les entreprises ont besoin d'un nombre toujours croissant d'informations nominatives.

Les traitements de données personnelles sont indispensables à la gestion des principales fonctions de l'entreprise : ressources humaines, gestion des rémunérations, suivi de la clientèle (comptes-clients, cartes de fidélité, service après-vente, mailings, établissement de profils de clientèle), marketing et prospection commerciale, relations publiques, recherche-développement, sécurité (contrôle de l'accès aux locaux et à l'information, vidéosurveillance). L'entreprise moyenne entretient donc plusieurs dizaines de bases de données nominatives.

De nombreux opérateurs économiques fondent aujourd'hui l'essentiel de leur activité sur le traitement et le transfert d'informations nominatives : banques, opérateurs de réseaux téléphoniques, compagnies aériennes (à travers la gestion des systèmes de réservation). Les données personnelles constituent les indicateurs de base des entreprises de services commerciaux. Elles leur permettent de développer une démarche de marketing personnalisé ***(****one to one*), dans un marché régi par une demande de plus en plus diversifiée.

Les bénéfices de cette évolution pour le consommateur sont indéniables. Il n'est plus le destinataire anonyme d'une publicité indifférenciée pour des produits de consommation de masse : la meilleure connaissance de ses besoins permet l'adaptation et la personnalisation de l'offre.

L'automatisation des instruments de gestion des relations avec la clientèle, la dématérialisation des opérations et l'utilisation des moyens de paiement électroniques, contribuent en outre à simplifier les transactions et à en réduire le coût. Le " porte-monnaie électronique " développé par La Poste permettra bientôt d'utiliser le paiement par carte, avec la même garantie d'anonymat que le règlement en espèce, pour la plupart des petites transactions.

Les bases de données personnelles constituent donc désormais un marché à part entière. Leur constitution et leur traitement sont l'élément principal de la valeur ajoutée produite par un grand nombre d'entreprises de services : vente par correspondance, agences de relations publiques, agences de casting, conseils en recrutement, entreprises de travail temporaire.

Certaines entreprises ont pour seule activité de collecter sur des questionnaires des informations sur les habitudes de vie, les centres d'intérêts et les goûts des personnes pour les céder à des tiers (*data warehouses* ou " magasins de données ").

Ce marché de l'information est soumis au droit de la concurrence, et le droit de commercialiser des données personnelles se rattache à la liberté d'entreprendre. Ces principes emportent des conséquences déterminantes.

En premier lieu, le champ du monopole des opérateurs publics sur certaines bases de données tend à se restreindre au bénéfice des opérateurs privés. Le droit de la concurrence en effet, dans de nombreuses matières, leur interdit de refuser de céder tout ou partie de ces données aux entreprises, et peut leur imposer d'ouvrir au secteur privé la faculté de constituer des fichiers concurrents.

En deuxième lieu, la liberté d'entreprendre des agents du marché de l'information s'étend à la collecte, au traitement, et à l'échange des données personnelles. Elle ne peut être restreinte que dans les limites strictement nécessaires à la protection des droits et libertés des personnes concernées.

Enfin, et c'est, avec la protection du droit des personnes, l'un des deux objet principaux de la directive du 24 octobre 1995 : la liberté de circulation des données doit être assurée entre les Etats membres de l'Union européenne. Cette liberté, afin de pouvoir s'exercer sans distorsion de concurrence, passe par l'harmonisation au sein de l'espace européen des garanties des droits et libertés des personnes concernées par les traitements.

L'informatique au service des libertés d'information et d'expression

Le traitement automatisé de données à caractère personnel constitue un puissant instrument au service de la liberté de la presse.

Il simplifie l'accès à l'information, tout en permettant une multiplication exponentielle du volume et des sources des données traitées.

Les journalistes travaillent aujourd'hui en liaison directe, dans le monde entier, avec les serveurs des agences de presse, les bases de données publiques, les archives informatisées des autres organes de presse et des grandes institutions.

La diversification des sources constitue une garantie de pluralisme et de fiabilité de l'information.

La possibilité pour les organes de presse de mettre leurs propres archives, en ligne, à la disposition du public, confère une nouvelle dimension de continuité à leur mission.

Enfin, la simplicité des modalités de transfert de données permet aux rédactions d'échanger et de diffuser instantanément des quantités presque illimitées d'informations, en faisant abstraction de toute barrière physique et politique. La presse télématique est appelée à jouer un rôle croissant pour la préservation d'un minimum de liberté et de continuité de l'information dans les pays où les médias ″ classiques " sont étroitement surveillés.

Mais la contribution de l'informatique à l'essor des libertés d'information et d'expression dépasse très largement le cadre de la presse. Le développement des réseaux permet en effet un changement de dimension dans les modalités d'exercice de ces libertés par chaque citoyen – dès lors qu'il dispose des équipements nécessaires.

Dans l'ordre de l'accès à l'information, l'internaute se trouve pratiquement à égalité avec les organes de presse : il peut interroger les mêmes sources, dans les mêmes conditions.

La numérisation des documents publics et leur diffusion sur les réseaux permettent de lever progressivement les dernières barrières matérielles à la liberté d'accès aux documents administratifs, et de conférer pleinement à ce qui n'était encore parfois qu'un droit formel le statut de liberté réelle. Les renseignements de tous ordres, les rapports publics, les textes juridiques, deviennent accessibles directement, en ligne. Il n'est plus nécessaire de formuler une demande ou de se rendre dans une administration pour les consulter.

L'impact des réseaux informatisés sur la liberté d'expression n'est pas moins considérable. Les forums contribuent à la multiplication et la diversification des espaces publics de discussion. Les sites publics, les sites thématiques ou les pages personnelles, confèrent aux citoyens de nouvelles capacités d'initiative et de participation à la vie démocratique. Le courrier électronique permet de diffuser instantanément une information ou un message à des destinataires multiples. Ces nouveaux instruments font apparaître, selon l'expression d'Herbert Maisl, les conditions d'une " démocratie électronique ".

Les évolutions technologiques confèrent enfin une nouvelle dimension à l'exercice collectif des libertés d'information et d'expression, dans la vie associative. Les réseaux offrent aux associations la possibilité d'accroître considérablement leur capacité de prospection et d'information, en disposant d'un accès instantané au public.

Le traitement de données personnelles au service de l'intérêt général

La gestion des services publics

Le développement des fichiers informatiques permet, à maints égards, de renforcer l'efficacité de l'action publique au bénéfice direct des administrés.

L'automatisation des procédures assure ***l'****égalité* et l'objectivité du traitement des administrés se trouvant dans une situation comparable au regard de l'exercice d'un droit ou d'une obligation – à condition qu'elle n'exclue pas la possibilité d'un examen des cas particuliers au regard des éléments suceptibles d'influencer la décision publique.

Ainsi, en matière fiscale ou sociale, le renforcement des instruments de lutte contre la fraude, trop souvent perçu comme porteur d'atteintes aux libertés, doit-il être regardé comme une garantie de l'égalité devant les charges publiques.

Le développement des traitements et des réseaux informatisés, dans la mesure où il permet une connaissance plus fine de la situation des administrés et de leurs besoins, induit une plus grande *adaptabilité* du service public aux attentes des citoyens. Il autorise un décloisonnement et une déconcentration des services, tout en maintenant une communication efficace avec les autorités centrales. L'évolution des moyens des administrations et des établissements publics, à cet égard, les rapproche des entreprises de service qui ont développé des relations de marketing direct avec leurs clients.

La mise en réseau des fichiers d'administrés – dès lors qu'elle ne conduit pas à détourner leur traitement de sa finalité – est de nature à garantir la *continuité* du service rendu par les divers opérateurs administratifs avec lesquels ils sont en relation, dans des cas où la multiplication et la dispersion des saisies d'informations sur papier peut mener à des incohérences – notamment lors des transmissions de dossiers en cas de changement de résidence, ou encore face à des demandes successives se rapportant à une même prestation.

L'informatisation permet enfin une *simplification* des procédures administratives et une accélération du traitement des dossiers. Les échanges de données informatisées ouvrent la voie aux téléprocédures, qui peuvent notablement simplifier les formalités à la charge des particuliers et des entreprises, en évitant notamment la multiplication des obligations déclaratives. La redistribution de l'information permettra par exemple de développer les dispositifs de " guichet unique " en matière d'emploi ou de prestations sociales.

La sécurité publique

Le traitement automatisé des données nominatives a considérablement accru la capacité et la

rapidité de l'information des services chargés de la protection de la sécurité publique, et ouvert un vaste champ – par l'intermédiaire des échanges de données – à la coopération internationale en la matière.

L'efficacité des nouveaux instruments est à la mesure des enjeux contemporains de la sécurité publique, notamment du développement d'une criminalité organisée à l'échelle internationale. Les bases de données automatisées sont indispensables à la lutte contre le terrorisme, contre les réseaux de trafic de stupéfiants, ou encore contre la grande délinquance financière.

En outre, l'automatisation des contrôles et le développement des échanges de données permet, tout en préservant le niveau des garanties de sécurité, d'alléger le poids des mesures nécessaires à la protection de l'ordre public : la mise en place d'un système commun d'information entre les Etats parties à la Convention de Schengen est le corollaire de l'allègement des contrôles physiques aux frontières entre ces Etats.

Enfin, de manière plus indirecte, la dématérialisation des procédures peut contribuer à réduire les facteurs de vulnérabilité à la délinquance. Une expérience-pilote d'introduction de cartes de paiement dans un lycée a ainsi permis d'y résorber le problème du rackett.

La santé publique

Les enjeux de l'automatisation du traitement de l'information en matière de santé sont considérables. Si la sensibilité des informations médicales impose que leur traitement soit soumis à une vigilance particulière, les progrès des technologies de l'information permettent de franchir de véritables sauts qualitatifs, aussi bien dans la garantie des droits individuels à la santé que dans une démarche globale de santé publique.

Dans l'ordre de la médecine curative, le développement des traitements automatisés et des échanges de données induira une grande simplification de l'accès aux soins. La carte Sésame-vital, appelée à remplacer la carte d'assuré social et le carnet de santé, permettra au praticien de disposer des informations de base sur le patient – désormais porteur de son dossier médical – et, par l'intermédiaire du réseau santé-social, de transmettre directement sa feuille de soins aux caisses d'assurance-maladie. A terme, le même réseau pourra faciliter l'échange de données sur un patient entre son médecin généraliste et les spécialistes ou l'hopital.

La mise en place de ces dispositifs doit évidemment s'accompagner d'un contrôle extrêmement vigilant des modalités d'accès aux données personnelles, dont le traitement, en matière de santé, revêt une sensibilité particulière. Le projet de réseau santé-social s'appuiera à cet égard sur un système de cryptologie, qui n'ouvrira l'accès à l'information sur chaque patient qu'à un destinataire déterminé, et qui – grâce à la carte professionnelle de santé – distinguera les niveaux d'habilitation des agents connectés au réseau. Le principe du colloque singulier entre le patient et le praticien se trouvera préservé par le fait que leurs deux cartes seront nécessaires à toute transmission d'information.

Dans l'ordre de la recherche scientifique, les bases de données informatisées sont aujourd'hui le support indispensable des études biomédicales, des travaux en matière génétique, ou encore du développement des produits pharmaceutiques. Le codage des données permet de garantir simultanément la fiabilité des échantillons et leur anonymat.

Le traitement automatisé des données médicales ouvre enfin de nouvelles dimensions aux politiques de santé publique.

Les échanges de données informatisées permettent des progrès considérables en matière épidémiologique, grâce à la mise en place de réseaux d'alerte et au suivi en temps réel de la

prévalence des pathologies.

Dans un contexte de contrainte financière, les dispositifs automatisés – comme ceux qui permettent d'asseoir la tarification hospitalière sur l'établissement de profils de patients (Programme Médicalisé des Systèmes d'Information) – garantissent une approche médicalisée de la maîtrise des dépenses de santé.

LES RISQUES

Le développement des applications qui viennent d'être présentées conduit à ce que chaque individu soit " fiché " plusieurs centaines, voire plusieurs milliers de fois. Toute personne est en effet appréhendée par des traitements automatisés de données dans une très grande diversité de situations : comme écolier, étudiant, salarié, contribuable, candidat à un emploi, patient, assuré social, bénéficiaire de prestations sociales, électeur, abonné au téléphone, à l'électricité et au gaz, locataire, titulaire d'un compte en banque, voyageur sur une ligne aérienne, abonné à un journal, client d'une librairie ou d'un supermarché, personne nominativement sondée sur ses jugements ou ses habitudes de consommation...

La collecte et le traitement de ces données se déroulent souvent à l'insu des intéressés, qu'il s'agisse de la mémorisation des données transactionnelles par l'informatique mobile (cartes à mémoire, téléphones cellulaires), de la conservation de traces informatiques lors du transit des données par des réseaux, ou encore de l'enregistrement de données par le biais de capteurs (caméras de vidéo-surveillance).

Les bénéfices, directs ou indirects, de ces traitements sont incontestables, dès lors qu'ils restent dans le cadre de finalités expressément définies.

Cependant, la multiplication et la diversification des données collectées, la facilité avec laquelle elles peuvent être transmises d'un opérateur à un autre, et les performances des logiciels d'analyse de données emportent de nombreux risques de détournements, qui sont susceptibles d'affecter la protection de la vie privée, de l'identité et des droits fondamentaux des personnes concernées.

Les atteintes à la vie privée

Que recouvre le droit au respect de la vie privée ?

La protection de la vie privée est au cœur des débats sur l'encadrement juridique des traitements de données à caractère personnel.

Ce que recouvre ce terme est cependant fort difficile à cerner. Alors même que la notion figure dans de très nombreux textes – article 8 de la Convention européenne des droits de l'homme , article 9 du code civil , loi du 3 janvier 1979 sur les archives, nouveau code de procédure civile – elle n'y est nulle part définie.

La jurisprudence ne fournit à cet égard que des indices qui – dans un ensemble donné de situations – permettent de dresser une typologie des composantes de la vie privée et des atteintes qui sont susceptibles d'y être portées.

Il en ressort que les éléments qui ont trait à l'individu et à sa vie familiale entrent dans le cadre de la vie privée, et qu'en revanche, les informations relatives au patrimoine et à la vie professionnelle ne bénéficient pas de la même protection.

L'article 9 du code civil protège en premier lieu l'individu dans les principaux traits qui dessinent son identité : nom, domicile, adresse (lorsqu'il en est fait une utilisation abusive), identité

physique (image de la personne saisie dans l'intimité de sa vie privée, santé), mœurs, identité sexuelle, opinions religieuses, philosophique, politique. Indépendamment de cette identité même, sont visées en outre les relations de la personne avec sa famille (mariage, divorce, naissance), ses proches, ses amis.

La protection est plus limitée en ce qui concerne les données patrimoniales et professionnelles. Si le patrimoine était regardé en toutes circonstances, jusqu'au début du vingtième siècle, comme un élément de la vie privée, la jurisprudence s'est sensiblement assouplie à cet égard, en considérant d'une part qu'il est licite de divulguer les éléments du patrimoine d'une personne occupant une place importante dans la vie publique et économique de la nation, d'autre part que le patrimoine ne constitue pas un élément de la vie privée lorsque sa divulgation ne s'accompagne pas de commentaires touchant à la personnalité ou à la vie même de l'intéressé.

S'agissant de la vie professionnelle, l'application de l'article 9 du code civil ne s'étend qu'à des cas très limités, comme l'enregistrement d'une conversation de l'intéressé à son insu. La protection de la vie privée ne saurait en revanche s'appliquer à la description de l'activité exercée, au contrat de travail, ni même à la dénonciation d'une faute ou d'une malversation commise dans un cadre professionnel.

La nature de l'information traitée ne suffit pas nécessairement à caractériser l'atteinte à la vie privée. Cette atteinte peut résulter d'une intrusion – c'est-à-dire de la collecte de données sans le consentement de l'intéressé –, mais aussi d'une utilisation abusive de l'information détournée de la finalité pour laquelle elle a été initialement collectée. Ainsi le traitement d'informations de santé – si sensibles soient-elles – ne soulève-t-il aucune difficulté lorsqu'il intervient dans le cadre des relations entre le patient et son praticien. Leur divulgation à un employeur peut en revanche constituer une atteinte caractérisée à la vie privée.

Certains paramètres, clairement établis, écartent la mise en jeu de la protection de la vie privée. C'est notamment le cas lorsque la divulgation de la vie privée résulte de l'application de dispositions législatives (quand elles permettent par exemple la collecte et le traitement d'informations par des moyens de vidéosurveillance), ou encore lorsque l'exploitation des informations en cause s'appuie sur le consentement clairement établi de la personne pour un usage déterminé (comme dans le cas d'un reportage autorisé par une personnalité).

La notion d'atteinte à la vie privée ne permet donc pas d'épuiser tous les cas de méconnaissance des droits des personnes auxquels la mise en œuvre de traitements de données à caractère personnel est susceptible de donner lieu :

–tout d'abord parce que la notion de " donnée à caractère personnel ", qui recouvre toute information susceptible d'être rapportée à une personne identifiée ou identifiable, est beaucoup plus large que celle de donnée relative à la vie privée,

–d'autre part en ce que le détournement des traitements de leur finalité, indépendemment de la nature des informations traitées, est susceptible d'emporter des atteintes à d'autres droits fondamentaux, comme les droits sociaux, où à la protection spécifique dont bénéficient certaines informations (secret médical, secret bancaire).

Les données sensibles

Il convient de souligner que toutes les informations relatives à la vie privée n'ont pas la même valeur, ni la même sensibilité.

L'utilisation d'informations relatives aux origines raciales, aux mœurs, aux opinions politiques, philosophiques et religieuses, ou aux appartenances syndicales, emporte des risques beaucoup

plus considérables que le traitement d'informations relatives à l'état-civil ou à la situation patrimoniale des personnes, notamment dans la mesure où elle met en jeu d'autres droits fondamentaux : la liberté d'opinion, la liberté de conscience, ou l'interdiction de toute discrimination en raison de ces caractères. Ces données sensibles, dont le champ est plus étroit que celui de la vie privée, doivent donc jouir d'une protection exceptionnelle. Leur traitement doit être regardé comme illégitime par nature, sauf dans des cas très particuliers, comme la tenue par les églises et les groupements à caractère religieux, philosophique et syndical de registres de leurs membres, ou pour des motifs d'intérêt public et sous réserve de garanties renforcées.

Le traitement des données médicales présente des risques comparables même si, contrairement aux cas qui viennent d'être énoncés, sa légitimité ne saurait être contestée. Leur utilisation doit être strictement limitée aux finalités de santé, de recherche et d'assurance-maladie.

Vie privée et liberté d'entreprendre

L'ampleur des risques d'atteinte à la vie privée varie toutefois selon la nature et l'objet des traitements de données mis en œuvre. Ces risques doivent être mis en balance avec les finalités des traitements.

Dans l'ordre des applications commerciales, le développement actuel du marketing personnalisé exige que l'on veille à un équilibre des intérêts. Certes, la concurrence entre les entreprises de commerce et de service aux particuliers leur impose une connaissance très précise de la demande, qui passe par un recensement toujours plus fin des comportements des consommateurs. La collecte et le traitement des informations personnelles à des fins commerciales – dont on a souligné plus haut les bénéfices directs pour le consommateur – emportent toutefois de nombreux risques pour les personnes concernées.

Le moindre est celui de voir leur boîte aux lettres saturée de prospectus publicitaires.

Les moyens techniques actuels permettent à ce démarchage de s'appuyer sur une connaissance très fine des comportements des consommateurs : les cartes de crédit et les cartes de fidélité permettent en effet de conserver la mémoire de l'ensemble des transactions réalisées par leur porteur, et d'en dresser un profil extrêmement précis.

Le développement d'internet, à cet égard, a démultiplié les possibilités de collecte d'informations, souvent à l'insu des utilisateurs du réseau. Le système des *cookies*, ou fichiers-témoins, créés automatiquement dans les ordinateurs clients, permet aux serveurs de conserver la trace de l'ensemble des sites visités par un internaute.

Faces à ces risques d'intrusion dans leur vie privée, les consommateurs doivent disposer d'un ensemble de garanties sur le recueil et le traitement d'informations les concernant, à chacun des stades de ces procédures :

–le droit de refuser d'être fiché ou prospecté,

–le droit d'être clairement informé sur les informations recueillies, sur les traitements dont elles sont susceptibles de faire l'objet et sur les finalités de ces traitements,

–le droit d'opposition à la communication des données à des tiers.

Les traitements qui viennent d'être évoqués procèdent de la même finalité générale que celle dans laquelle les données ont été recueillies. La circonstance que ces données aient été enregistrées dans le cadre d'une transaction commerciale n'autorise cependant pas pour autant l'entreprise qui les collecte à en faire usage à des fins de prospection sans information préalable de la personne concernée, et encore moins à les céder à d'autres opérateurs.

Beaucoup plus dangereuse, compte tenu des facilités existantes en matière de transfert de données, est la faculté d'utiliser des données à des fins radicalement différentes de celles pour lesquelles elles ont été collectées.

Pour prendre un exemple extrême, la communication de certaines données de santé à un assureur ou un banquier, peut conduire à des discriminations et à des exclusions inadmissibles. Ainsi, la répercussion encore trop souvent négative de la connaissance de l'état d'infection par le virus HIV sur la vie professionnelle ou sociale des personnes concernées impose-t-elle une particulière vigilance à l'égard de la constitution et du traitement de fichiers comportant ce type de données.

Vie privée et intérêts publics

La question du détournement de finalité du traitement de données relatives à la vie privée se pose avec une acuité particulière dans le cas des applications mises en œuvre par les autorités investies de missions de service public.

Celles-ci ont en effet, en vertu de la loi, le droit d'accéder à des informations protégées par le secret de la vie privée ou par d'autres dispositions. Ce droit s'exerce dans le cadre de finalités déterminées : le secret bancaire peut être levé pour la recherche des infractions fiscales ou au cours d'une procédure judiciaire, et certaines informations relatives à la vie privée doivent être communiquées aux caisses de sécurité sociale pour bénéficier des prestations qu'elles dispensent.

L'accès des administrations à ces informations doit en conséquence être strictement encadré et contrôlé. Ainsi, l'ouverture de certains services ou prestations à l'ensemble des personnes résidant en France, y compris les étrangers en situation irrégulière, serait privée de toute portée si les informations nécessaires à leur bénéfice étaient communicables aux services de police.

Le champ des informations susceptibles d'être traitées pour une finalité donnée doit être clairement délimité, et les échanges d'informations ou les interconnexions de fichiers, dans le cadre de procédures répondant à des finalités distinctes, doivent être encadrés par les textes.

Les atteintes à l'identité des personnes

Le champ des données susceptibles d'être recueillies et transmises sur chaque individu, à l'ère pré-informatique, était étroitement circonscrit, et se réduisait le plus souvent à des informations incontestables telles que son état-civil, sa profession ou son adresse. Les opérateurs qui en disposaient étaient identifiables, chaque communication étant l'occasion d'une formalité (changement d'adresse, fourniture de documents d'état-civil, renseignement d'un formulaire).

L'évolution technique étend presque à l'infini le nombre des données personnelles susceptibles d'être recueillies et traitées, souvent à l'insu des personnes concernées, et les facultés de transmission de ces données entre les opérateurs.

a) La " carte d'identité " dont disposent les administrations, les employeurs, les fournisseurs, peut désormais comporter des centaines de rubriques, dont la maîtrise échappe de plus en plus largement aux personnes concernées.

L'attention de la mission a ainsi attirée sur la constitution, aux Etats-Unis, de vastes bases de données personnelles concernant les cadres et les ingénieurs de haut niveau, destinées à une clientèle internationale de cabinets de conseil en recrutement. Leur existence avait été révélée à l'un de ces ingénieurs par une série d'échecs à des entretiens d'embauche, liés à la diffusion à l'ensemble des entreprises approchées de données inexactes sur son curriculum vitae. Dans un nombre croissant de situations, l'individu peut ainsi se trouver dans l'ignorance de la collecte et du traitement de données susceptible d'emporter une influence déterminante sur sa situation

personnelle.

Ce n'est pas la vie privée qui est ici en cause, s'agissant d'informations à caractère purement professionnel. En revanche, c'est son identité – définie par la Commission nationale de l'informatique et des libertés (C.N.I.L.) comme " ce qui permet de distinguer une personne d'une autre ", au sens large (avis du 9 juin 1981 sur le répertoire national d'identification des personnes) – qui se trouve atteinte. La protection de l'identité des personnes implique cependant que celles-ci disposent d'une information et d'un droit de regard sur la collecte et le traitement d'informations le concernant, afin de pouvoir, le cas échéant, obtenir la rectification ou l'effacement de données erronnées, particulièrement lorsqu'elles sont susceptibles d'affecter ses droits.

b) Définie dans une acception plus stricte par le même avis de 1981 de la C.N.I.L., l'identité recouvre ce qui permet de dénommer une personne, c'est-à-dire de la distinguer d'une autre de façon non équivoque. Etaient principalement visés dans le contexte technique de l'époque les identifiants numériques, et au premier chef le numéro d'identification au répertoire national (NIR) mis en place par l'INSEE, dont l'utilisation fait l'objet d'un encadrement très vigilant.

Les inquiétudes suscitées dans l'opinion par cet identifiant universel remontent à sa création, et se rattachent à des causes diverses.

En premier lieu, alors que, dans d'autres pays européens (Royaume-Uni, Espagne), ce numéro est déterminé de manière aléatoire, il est, en France, porteur d'informations sur l'état-civil de la personne (sexe, date et surtout lieu de naissance). Il permet donc en théorie d'opérer une sélection discriminante entre diverses catégories de la population, sur la seule base des informations qu'il comporte (comme la naissance à l'étranger). Ce risque s'est réalisé dans l'administration du régime de Vichy, qui avait inclus dans l'identifiant des données sur l'origine des personnes.

En deuxième lieu, l'identifiant national a longtemps été la clé de l'interconnexion entre les fichiers publics, dans la mesure où il apparaissait comme le seul instrument permettant la distinction des personnes sans risques d'homonymie. L'émotion suscitée par le projet SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus), qui visait à permettre, à partir de ce numéro, l'interconnexion des grands fichiers publics, est pour une large part à l'origine de la loi sur l'informatique et les libertés. Les risques de détournement de finalité qu'emporte une interconnexion sans contrôle ont été soulignés plus haut.

Il convient toutefois de préciser que, dans le contexte technique actuel, ce risque n'est plus spécifique aux identifiants numériques. De puissants moteurs de recherche permettent aujourd'hui, à partir d'interrogations multicritères (par exemple nom et adresse, ou nom et date et lieu de naissance), d'établir très rapidement une correspondance sans équivoque entre deux fichiers en se passant de ces identifiants. Les logiciels d'identification vocale et visuelle permettront bientôt de parvenir au même résultat à partir de la voix et de l'image.

Enfin, et de façon plus diffuse, la méfiance à l'égard de l'identifiant national procède du refus des citoyens d'être réduits à des numéros dans leurs relations avec l'administration. La crainte de perdre son nom, profondément ancrée dans les mentalités, est au cœur du problème de la protection de l'identité des personnes dans le cadre des traitements de données personnelles. Ce motif avait conduit Alfred Sauvy, au moment où l'administration de Vichy travaillait à la conception de l'identifiant national, à s'opposer à son extension.

c) Les risques liés au numéro national, on vient de le souligner, ne lui sont plus spécifiques, en raison de la diversification des identifiants exploitables et de l'amélioration des performances des

instruments de recherche.

L'exemple ultime, et celui qui présente les plus grands risques, est constitué par les collections d'échantillons biologiques réunies à des fins d'études génétiques (cf. Axel KAHN, " La recherche en génétique humaine : collecte et conservation d'échantillons biologiques et de données ", *Actes des journées annuelles d'éthique, Génétique et médecine*). Ces échantillons contiennent en puissance un ensemble considérable d'informations d'une grande sensibilité, puisqu'ils peuvent donner accès à certains aspects sensibles du destin des individus et de leur lignage. Leur utilisation peut donner lieu à bien d'autres recherches que celle qui était initialement imaginée lorsque l'auteur de la collection l'a réunie, dans un sens qui peut heurter les convictions intimes du donneur de l'échantillon. Le traitement de données biologiques aussi intimement constitutives de son identité – et de celle de membres de sa famille – doit donc être entourée de garanties : le droit d'être informé des buts de l'enquête aux fins de laquelle les échantillons ont été prélevés, ainsi que des finalités de toute enquête ultérieure, le droit de sortir de l'étude et de demander qu'un échantillon les concernant soit détruit.

Les risques liés à l'automatisation de la prise de décision

Le problème de la protection de l'identité des personnes recoupe partiellement celui des risques liés à l'automatisation de la prise de décision ou du traitement des informations qui en sont le support.

Le refus d'être identifié par un simple numéro emporte également celui d'être réduit à un " profil " de personnalité ou à un " segment " comportemental dans les relations avec l'administration et avec les organismes privés dont les décisions peuvent affecter de façon significative la situation d'une personne.

L'automatisation de la prise de décision est en effet susceptible, en elle-même, de porter atteinte à certains droits de la personne, comme le droit à un examen particulier de son cas, les droits de la défense, ou l'exigence de motivation des décisions défavorables.

Ces droits bénéficient de solides garanties législatives et jurisprudentielles dans les relations entre l'administration et les citoyens : toute personne faisant l'objet d'une décision négative a droit à un examen particulier de son cas, et doit être mise à même de présenter ses observations et informée des motifs de la décision prise à son encontre. Ces garanties doivent être préservées face au développement de l'automatisation des décisions publiques – notamment en matière fiscale et sociale – sans pour autant contrecarrer un processus qui contribue à améliorer l'efficacité du service public.

Les administrés doivent, au minimum, pouvoir connaître les critères pris en compte à l'appui de décisions automatisées, et avoir la faculté de demander un réexamen de leur cas particulier en dehors de tout cadre " mécanique " et dans des conditions qui leur permettent de faire valoir leur point de vue.

Ces droits doivent également s'appliquer aux décisions d'organismes privés qui produisent des effets juridiques à l'égard des personnes, ou qui les affectent de manière significative, comme celles des employeurs relatives à la situation de leurs salariés, celles des établissements bancaires en matière de crédit ou certaines décisions des compagnies d'assurances.

De manière plus grave, le développement des échanges de données et l'automatisation du traitement des informations qui servent de support aux décisions affectant la situation des personnes peuvent faciliter la prise en compte de critères illicites à l'appui de ces décisions.

La question du détournement de la finalité des traitements a été évoquée plus haut, en tant qu'elle

était susceptible de porter atteinte à la vie privée. Plus fondamentalement, elle peut affecter l'impartialité de l'auteur de la décision et emporter des discriminations illégales. Un exemple extrême, à cet égard, est fourni par la prise en compte du critère de l'origine raciale des personnes dans l'élaboration du premier numéro national d'identification par le régime de Vichy. Dans le contexte actuel, la multiplication des informations traitées et la facilité de leur transmission peuvent conduire à des discriminations dans des domaines où le principe d'égalité a vocation à s'exercer, comme l'accès à l'emploi, au logement, ou aux prestations d'aide sociale.

LA MAITRISE DU PROGRES

L'identification des risques liés au développement du traitement automatisé d'informations nominatives a conduit le législateur, dans la plupart des pays occidentaux, à délimiter des droits d'un type nouveau – que l'on pourrait désigner par l'expression simplificatrice de " droits de la personne fichée " :

–la garantie que la collecte d'informations la concernant ne sera pas opérée par des moyens frauduleux ou déloyaux ;

–le droit de s'opposer, pour des raisons légitimes – et sous réserve de certaines exceptions – à ce que des informations nominatives la concernant fassent l'objet d'un traitement ;

–le droit d'être informée de la destination des informations recueillies auprès d'elle ;

–la garantie que ces informations ne seront pas déformées, endommagées ou communiquées à des tiers non autorisés ;

–le droit d'accéder à ces informations et, si elles sont inexactes, de demander leur rectification, leur mise à jour ou leur effacement ;

–le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.

La spécificité et la nouveauté de ces droits a conduit le législateur, dans l'ensemble des pays qui ont adopté une législation protectrice, à confier le contrôle de leur application – au premier niveau – à une autorité spécialisée plutôt qu'au juge.

Cette fonction a été assurée en France par la Commission nationale de l'informatique et des libertés, dont l'intervention a permis de dégager des règles cohérentes d'application des principes qui viennent d'être énoncés et de les adapter au développement rapide des technologies de l'information qui a marqué les deux dernières décennies.

Ces règles et ces contrôles sont trop souvent appréhendées par certains responsables de traitements comme des entraves au développement des moyens informatiques dans l'administration et dans l'entreprise. Mais, de même que le code de la route n'a pas tué l'automobile, l'encadrement juridique du traitement des données personnelles a été l'instrument d'une indispensable maîtrise des progrès des technologies de l'information.

La protection des droits des " personnes fichées " se confond en effet, dans le long terme, avec celle du développement de l'informatique. La législation sur l'informatique et les libertés, en ce qu'elle a permis d'apaiser les craintes des citoyens, des consommateurs et des groupes sociaux, a contribué à la diffusion des technologies de l'information dans la société française. En facilitant l'acceptation des progrès irréversibles de l'informatique, la loi de 1978 a contribué à les rendre plus familiers aux citoyens.

La portée considérable des évolutions intervenues dans ce domaine, depuis vingt ans, doit

cependant conduire à reconsidérer les modalités de l'encadrement et du contrôle du traitement des données personnelles.

La possibilité de transmettre instantanément des données d'un point du globe à un autre, et le développement de réseaux universels, rendent vaine toute démarche de protection qui se limiterait à un cadre strictement national. En effet, des disparités trop sensibles entre les réglementations nationales peuvent inciter les opérateurs à délocaliser les traitements et les bases de données dans des " paradis informatiques " qui leur opposeraient moins d'entraves. La nécessité d'une harmonisation des niveaux de protection dans l'Union européenne est à la source de l'initiative française qui a abouti à la directive du 24 octobre 1995. Cette démarche doit être prolongée par une négociation à l'échelle mondiale, afin d'éviter que les risques qui viennent d'être énoncés ne se reportent aux frontières de l'Europe.

La diffusion de puissants instruments de traitement automatisé de l'information dans les entreprises et chez les particuliers a contribué a réduire la spécificité des applications mises en œuvre par les opérateurs publics.

Dès lors, la différenciation des règles applicables aux traitements selon qu'ils sont ou non opérés pour le compte d'une personne morale de droit public – sauf dans des domaines très particuliers comme la protection de la sécurité publique – a perdu une large part de ses justifications.

La banalisation des traitements doit en outre conduire à plus clairement prendre en compte les droits du citoyen, non seulement comme " personne fichée ", mais de plus en plus comme usager ou comme responsable d'un traitement. Le droit de l'informatique tendra en effet de façon croissante à se confondre avec le droit commun des procédures administratives et des relations commerciales. Dans ces conditions, les technologies de l'information sont appelées à devenir, sinon le vecteur principal, du moins un support essentiel de l'exercice des libertés d'expression et d'information et de la liberté du commerce et de l'industrie. Il y a lieu de tenir compte de ces évolutions fondamentales pour définir un nouvel équilibre entre la protection des droits de la " personne fichée " et ceux des opérateurs des traitements d'informations.

Première partie

DU DROIT NATIONAL A LA DIRECTIVE EUROPEENNE

Chapitre I

LE DROIT APPLICABLE EN FRANCE

Section 1 : LA LOI DE 1978

Genèse

À la fin des années soixante, en Europe comme aux Etats-Unis et au Canada, de nombreux travaux relatifs au développement de l'informatique dans l'administration viennent souligner les risques que la technique informatique semble faire peser sur les libertés publiques. Ces réflexions et discussions émanent pour la plupart de l'appareil gouvernemental ou de la Haute administration des Etats eux-mêmes et les premiers textes législatifs apparaissent rapidement.

En octobre 1970, le Land de Hesse adopte la première loi relative au " traitement automatisé des informations nominatives " qui jettera les fondements de la loi fédérale de novembre 1976. Entre-temps, en mai 1973, le parlement suédois adoptera lui aussi une loi sur le traitement automatisé des informations nominatives. De leur côté, en janvier 1974, les Etats-Unis se dotent d'un *Privacy Act* dont l'application est limitée aux fichiers détenus par les administrations fédérales et qui est destiné à protéger la vie privée des individus contre l'utilisation abusive

d'enregistrements détenus par ces administrations en permettant à chacun d'accéder aux enregistrements qui le concernent.

Si l'on ne peut négliger ce contexte ni les multiples contributions écrites, notamment de la part de la science administrative, il semble néanmoins qu'en France, le fait générateur de la loi de 1978 réside dans la révélation au public non seulement de plusieurs projets concomitants, dont celui bien connu sous le nom de SAFARI, mais aussi, et même surtout, des conditions particulièrement obscures dans lesquelles ces projets sont élaborés, conditions qui tranchent précisément avec le thème alors fédérateur de la transparence administrative et du respect, par les Etats, de la vie privée de leurs citoyens.

En 1970, l'INSEE décide, semble-t-il de son propre chef, d'informatiser le répertoire d'identification et le numéro national d'identification de tous les Français. Ce répertoire, et le numéro qu'il contient, avaient été créés par le " Service de la démographie " au printemps 1941, à partir des relevés des registres des actes de naissance généralement effectués par les greffiers des tribunaux de première instance (instructions du 18 mars et du 11 avril 1941). Le but de cette informatisation était de parvenir à un identifiant unique pour les fichiers de toutes les administrations publiques et les caisses de la Sécurité sociale.

Dans le même temps, le ministère de l'Intérieur s'apprêtait à mettre en œuvre un ordinateur très puissant destiné à la centralisation des bases de données que possédaient les services de police (dont les renseignements généraux, la direction de la sécurité du territoire, la police judiciaire).

Or, le paradoxe que révélait l'article de Philippe Boucher (" Safari ou la chasse aux Français, paru dans *Le Monde* le 21 mars 1974) était que le Premier Ministre avait écarté toute proposition de débat public sur les projets d'informatisation du gouvernement et ce, contrairement aux recommandations du Conseil d'Etat (rapport non publié de 1971) ou du ministère de la Justice mais contrairement aussi aux gouvernements des pays voisins.

L'émotion suscitée fut suffisamment vive pour le que Premier Ministre interdise aux services de procéder sans son autorisation à de nouvelles interconnexions et demande au Garde des Sceaux, par décret en date du 8 novembre 1974, de constituer une commission chargée de " proposer au Gouvernement, dans un délai de six mois, des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques ". Présidée par le vice-président Chenot, cette commission remettait le 27 juin 1975 un rapport rédigé par M. le Conseiller Bernard Tricot, Rapporteur général et M. le Professeur Pierre Catala. La publication de ce rapport par la Documentation française a contribué à éclairer les termes du débat.

C'est sur le fondement de ces travaux que fut élaboré un projet de loi déposé le 9 août 1976, dont le Parlement eût à débattre dès le 4 octobre 1977 et qui aboutit à la loi du 6 janvier 1978 que nous connaissons.

Au début des années 80, la multiplication des lois comparables en Europe – la Norvège adopte une loi sur les registres de données personnelles en 1978 – suscitera quelques réactions au plan international, certains Etats craignant en effet que les législations sur la protection des données n'entravent la libre circulation de ces dernières et les échanges commerciaux dont elles font l'objet. Des discussions s'engagent au sein de l'OCDE qui arrête des Lignes Directrices, en date du 23 septembre 1980. Dénuées de toute force obligatoire, ces Lignes reprenaient les principes essentiels des législations nationales, mais leur objectif était justement d'éviter que la protection des données personnelles ne crée des obstacles injustifiés à la libre circulation de l'information entre les pays membres et au développement des relations économiques et sociales entre ces pays. La Convention 108 du Conseil de l'Europe, signée à Strasbourg le 28 janvier 1981 s'inscrit,

elle aussi, dans ce processus comme en témoigne le dernier alinéa de son Préambule qui évoque " la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples ".

Il y avait donc, dès l'origine, deux points de vue, certes compatibles mais correspondant néanmoins à deux sensibilités différentes. Tandis que les droits français, allemand ou suédois d'un côté, faisaient de la protection de l'individu face aux dangers de l'informatique une fin en soi, le droit international et européen faisait de cette protection la contrepartie du principe de libre circulation de l'information.

Contenu

Champ d'application

Le champ d'application de la loi du 6 janvier est déterminé par les définitions qu'elle-même donne de certains concepts fondamentaux dont celui de traitement automatisé d'informations nominatives (article 5). Sont donc concernées en premier lieu les données nominatives qui ont fait l'objet d'un traitement automatisé. Ces données sont soumises à toutes les dispositions de la loi.

À côté de celles-ci, il convient de distinguer les données nominatives qui ont fait l'objet d'un traitement non automatisé au sein d'un fichier se rapportant à l'exploitation de fichiers ou bases de données. En effet, le projet de loi ne prévoyait pas d'inclure les fichiers manuels qui doivent leur intégration à un amendement parlementaire. Quoi qu'il en soit, l'article 45 étend le champ d'application de la loi à ces fichiers mais de façon limitée : seules leur sont applicables certaines dispositions de la loi.

Enfin, le champ d'application des dispositions applicables aux fichiers manuels ou mécanographiques est susceptible d'être modifié, selon la procédure prévue à l'alinéa 4 de l'article 45, par décret en Conseil d'Etat sur proposition de la CNIL. Mais cette disposition n'a jamais été appliquée à ce jour.

Les principes

Les règles énoncées par la loi du 6 janvier reposent sur certains principes essentiels :

–le principe de la protection de la vie privée semble justifier l'idée que tout traitement automatisé doit conserver un caractère supplétif ou fonctionnel. C'est ce principe que nous semble contenir l'article premier, lequel dispose que l'informatique doit être au être au service de chaque citoyen, ainsi que l'article 2 qui prévoit qu'un traitement automatisé donnant une définition du profil ou de la personnalité de l'individu ne peut justifier à lui seul une décision de justice, administrative ou privée. C'est enfin probablement ce principe qui caractérise le plus la différence de point de vue entre la loi française et les dispositions de l'OCDE et du Conseil de l'Europe ;

– le principe de transparence fonde l'essentiel des droits que consacre la loi en matière d'accès, d'opposition, de communication ou de rectification ;

–le principe du droit à l'oubli et au secret ou à la confidentialité, enfin, justifie que tout traitement soit limité dans le temps et que les données qu'il contient et gère soient protégées et régulièrement mises à jour.

Si la loi ne fait pas expressément mention du principe de finalité, elle en fait une application partielle en imposant que soit indiquée la finalité du traitement dans les déclarations (article 19) et en sanctionnant pénalement le détournement de finalité (article 226-21 du nouveau code pénal).

Les règles et les droits

La loi établit une première distinction, que l'on peut qualifier d'organique, entre les traitements du secteur public et ceux du secteur privé : les premiers doivent faire l'objet d'une autorisation préalable de la CNIL (article 15), les seconds doivent simplement lui être déclarés (article 16). C'est cette *summa divisio* que remet en cause la directive européenne d'octobre 1995.

Mais la loi établit une seconde distinction, matérielle cette fois, entre les données. Certains traitements qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, parce qu'ils relèvent de pratiques courantes, peuvent faire l'objet d'une simple déclaration de conformité aux normes simplifiées de la CNIL (article 17). En revanche, à l'opposé, les traitements portant sur 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 sont interdits (article 31).

Bien que l'expression ne figure pas dans la loi, cette dernière consacre certains droits au profit des " personnes fichées ". Il n'en reste pas moins que la liste de ces droits varie selon les auteurs. Semble toutefois hors de doute l'existence d'un droit d'accès, de communication et de rectification, respectivement prévus par les articles 34, 35 et 36. Le premier ne requiert aucune motivation spécifique – sinon celle d'être une personne physique et non morale, compte tenu de l'article 4 de la loi – et consiste littéralement en un droit à l'interrogation des services chargés de mettre en œuvre des traitements. Le deuxième semble découler du premier : l'accès n'a de sens qu'à la condition de pouvoir obtenir communication des informations en question. Enfin, le dernier achève la construction : les informations doivent pouvoir être rectifiées. Certains auteurs ont considéré que la loi consacrait un droit à l'effacement des données, conséquence d'un droit à l'oubli. Ce serait pourtant omettre que l'alinéa 1 de l'article 36 prévoit une gradation dans l'échelle des mesures valant rectification, échelle à l'extrémité de laquelle figure, précisément, l'effacement de données dont la collecte et le traitement sont interdits.

À ces droits, l'on peut en ajouter d'autres : d'une part, le droit d'opposition qui figure à l'article 26 lequel, doit-on préciser, n'impose pas en retour que le consentement de la personne dont on collecte les données personnelles soit préalablement recueilli ; et d'autre part, la garantie de la qualité des données collectées (article 29).

L'autorité de protection

La popularité de la loi de 1978 tient certes à l'attachement des citoyens aux droits qu'elle protège mais également au fait qu'elle fut la première à consacrer la notion d'autorité administrative indépendante.

Placée au centre du dispositif législatif, la CNIL est composée de dix-sept membres nommés pour cinq ans ou pour la durée de leur mandat. On sait que sa composition donna lieu à un âpre débat au Parlement et que le projet, qui ne prévoyait la présence d'aucun parlementaire, fut modifié sur ce point.

La CNIL compte deux députés et deux sénateurs, deux membres du Conseil économique et social, deux membres du Conseil d'Etat, deux membres de la Cour de Cassation, deux membres e la Cour des comptes, deux personnes qualifiées pour leur connaissance des applications de l'informatique et trois personnalités désignées en raison de leur autorité et de leur compétence. La CNIL dispose également de services administratifs. Enfin, siège auprès d'elle un commissaire du gouvernement dont la présence n'entame en rien l'indépendance de la Commission : chargé de tenir informé le Premier ministre, il a pour seul pouvoir de provoquer une seconde délibération dans les dix jours d'une délibération (article 9).

Outre ses pouvoirs d'autorisation des traitements publics, sa mission d'enregistrement des traitements privés, de contrôle *a posteriori* et son pouvoir d'édicter des normes simplifiées, la CNIL est, de par la loi, investie d'un rôle d'information du public grâce à la publication de son Rapport annuel et d'un rôle consultatif non négligeable auprès des personnes qui souhaitent créer un traitement automatisé d'informations nominatives.

Dans toutes ces fonctions, la CNIL a toujours su, de l'avis général, faire la preuve de son indépendance.

Les mesures d'application

Décrets et arrêtés

L'application de la loi du 6 janvier a donné lieu à l'édiction de nombreux textes réglementaires.

Décret no 78-774 du 17 juillet 1978 pris pour l'application des chapitres I à IV et VII.

Décret no 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publique de la loi du 6 janvier 1978.

Décret no 81-1142 du 23 décembre 1981 instituant des contraventions de police en cas de violation de certaines dispositions de la loi du 6 janvier 1978.

Décret no 85-525 du 16 juin 1982 relatif à la redevance prévue à l'article 35 al. 2 de la loi du 6 janvier.

Arrêté du 23 septembre 1980 relatif à l'homologation d'une décision de la CNIL fixant le montant de la redevance perçue à l'occasion de la délivrance de copies d'informations nominatives faisant l'objet de traitements automatisés.

Décret no 82-103 du 22 janvier 1982 relatif au RNIPP.

Décret no 85-420 du 3 avril 1985 relatif à l'utilisation du RNIPP par des organismes de sécurité sociale et de prévoyance.

Décret no 91-1404 du 27 décembre 1991 autorisant l'utilisation du RNIPP par les employeurs dans les traitements automatisés de la paie et de la gestion du personnel.

30 décrets pris en application de l'article 18 (utilisation du RNIPP).

Règlements intérieurs

La CNIL a arrêté son règlement intérieur par délibération no 87-25 en date du 10 février 1987 lequel a été modifié à deux reprises : délibérations no 92-087 du 22 septembre 1992 et no 93-048 du 8 juin 1993).

Normes simplifiées

Conformément à l'article 17, la CNIL est investie d'un pouvoir réglementaire limité l'autorisant à établir des normes simplifiées. C'est là l'une une autre originalité de la loi de 1978 dont l'origine est parlementaire. On la doit très exactement à l'amendement no 69 de M. Raymond Forni, que la Commission avait d'ailleurs repris à son compte (amendement no 113) (*JO*, *AN*, Séance du 5 octobre 1977, p. 5850) : " Il s'agit, expliquait M. Forni, de fixer certaines normes pour les catégories de fichiers les plus courantes, ce qui ne devrait soulever aucune opposition ". Effectivement, l'amendement fut adopté sans discussion. Le Sénat n'y revint pas. À l'époque, nul

ne songea à soulever le problème de la conformité à la Constitution de ce pouvoir réglementaire accordé à la CNIL.

La première norme simplifiée élaborée par la CNIL, en date du 22 janvier 1980, concernait les traitements automatisés d'informations nominatives relatifs à la liquidation et au paiement des rémunérations des personnels de l'Etat.

Elle fut suivie de 39 autres normes.

Une seule fut annulée par le Conseil d'Etat.

Section 2 : LES LOIS SPÉCIFIQUES

La loi du 6 janvier 1978 est sans doute le texte fondateur et primordial de la protection des données à caractère personnel. Mais, contrairement à une opinion assez répandue, elle n'épuise pas le sujet. Une trentaine d'autres lois sont intervenues depuis lors dans ce domaine et le rythme s'accélère (vingt dans les dix dernières années, parfois jusqu'à trois ou quatre par an). Il est utile d'en faire un recensement (voir liste en annexe) et une analyse.

Domaine

Le législateur de 1978 a bien senti que certains fichiers et traitements relèvent par nature du domaine de la loi. Il l'a montré dans une réserve qui se trouve au début de l'article 15 relatif à la mise en œuvre des traitements par les autorités publiques : " hormis les cas où ils doivent être autorisés par la loi ". Un amendement parlementaire avait eu pour objet de préciser ces cas. Mais le Garde des Sceaux a objecté qu'il n'appartenait pas à une loi de modifier la Constitution et l'amendement a été rejeté. Il faut observer que le texte comporte le mot " doivent " parce qu'à l'époque les limites posées au domaine de la loi étaient impératives, alors que peu de temps après, en 1982, le Conseil Constitutionnel a admis que la législateur pourrait intervenir dans des domaines qui ne lui sont pas réservés. Ce qui demeure, c'est que selon l'article 34 de la Constitution, certaines règles ne peuvent être posées que par la loi. Lesquelles ?

" L'état des lieux " révèle dans ce domaine une doctrine implicite et pour ainsi dire " instinctive ", qu'il conviendrait de préciser à l'avenir, mais aussi des incohérences et des contradictions qu'il faudrait éviter.

Contenu

Ce désordre apparaît également dans les dispositions de ces lois, qui, non seulement couvrent des domaines divers, mais encore ont des formes et objets très différents.

On peut d'abord relever des *différences de pure forme*, qui sont sans doute inévitables en l'état de notre droit et de nos techniques législatives. Tantôt ces textes constituent à eux seuls une loi, comme celles de 1980 sur le casier judiciaire, de 1990 sur les permis de conduire, de 1994 sur les recherches en matière de santé, tantôt ils ne sont que l'une de ces dispositions d'ordre social ou financier qui coexistent, dans une loi " fourre-tout ", avec des règles ayant un tout autre objet. Parfois, ces dispositions sont introduites dans des codes comme ceux de la santé publique, de la sécurité sociale ou du travail, ou viennent modifier un texte ancien comme le décret-loi du 30 octobre 1935 sur les chèques.

Ces textes ont également des *objets* différents et variés :

–transmission d'informations entre des organismes de sécurité sociale et des services administratifs et fiscaux (loi du 10 mai 1993) ou entre des administrations (loi du 3 juin 1985) ;

–accès des organismes de sécurité sociale aux fichiers de police pour vérifier la situation administrative des étrangers (loi du 24 août 1993) ;

–création de fichiers ou de traitements automatisés d'informations (lois du 30 décembre 1989 sur le surendettement, du 19 décembre 1991 sur le permis de conduire, du 31 décembre 1991 sur les incidents de paiement) ;

–déclarations uniques destinées à plusieurs services, pour faciliter, les relations entre l'administration et les usagers (loi du 3 janvier 1985) ;

–utilisation du registre national d'identification des personnes physiques, qui relève pourtant, selon l'art. 18 de la loi de 1978, du décret en Conseil d'État après avis de la C.N.I.L. (loi du 4 février 1995).

Récemment encore, au printemps de 1997, le gouvernement avait préparé un projet de loi relatif à l'interconnexion de fichiers sociaux et fiscaux, qui n'est pas venu en discussion au Parlement en raison de la dissolution de l'Assemblée nationale.

Certaines lois ont un caractère négatif. Ainsi la loi du 9 juillet 1991 sur les procédures civiles d'exécution dispose que " les renseignements obtenus ne pourront en aucun cas être communiqués à des tiers ni faire l'objet d'un fichier d'informations nominatives ".

Il est remarquable qu'aucune de ces lois n'exige que l'accès ou l'interconnexion des fichiers ou des traitements soient limités à ceux qui ont été régulièrement autorisés et qu'il n'ait jamais été envisagé que cette condition ait été implicite.

Les renvois ou références à la loi de 1978 se caractérisent également par leur diversité. On peut à cet égard distinguer quatre catégories de solutions, sans que la justification de ces différences apparaisse clairement :

–renvoi global pur et simple à la loi de 1978 ;

–renvoi à certains articles de cette loi, notamment l'article 15 sur la procédure préalable, les articles 35 et 36 sur les droits d'accès et de rectification et les dispositions pénales ;

–établissement d'une procédure spéciale comportant l'avis simple de la C.N.I.L. sur les règlements d'application de la loi, ou, à l'inverse, une décision d'autorisation délivrée par la C.N.I.L. ;

–utilisation de formules obscures telles que " la présente loi ne fait pas obstacle " à l'application de celle de 1978, ou " sans préjudice " des dispositions de la loi de 1978 ;

–enfin, absence référence tant à la loi de 1978 qu'à à la C.N.I.L., ce silence valant soit référence globale implicite, soit, au contraire, exclusion de la loi générale par la loi spéciale.

Une dernière catégorie, également radicale mais en sens opposé, est constituée par une seule loi : les auteurs de la loi du 1er juillet 1994, qui était l'une des lois dites de bioéthique et qui constituait un texte largement dérogatoire, l'ont incorporée directement dans la loi de 1978, dont elle constitue le chapitre V bis.

Section 3 : LE DISPOSITIF PÉNAL

La législation pénale française applicable en matière de protection des personnes à l'égard des traitements automatisés de données nominatives résulte tant de la loi du 6 janvier 1978 elle-même, modifiée par la loi du 16 décembre 1992, que du Code Pénal.

La loi de 1978 modifiée comporte deux délits prévus par les articles 42 et 43, soit l'utilisation du répertoire national d'identification des personnes physiques sans les autorisations prévues par la loi, punie de 5 ans d'emprisonnement et 500 000 F d'amende, et l'entrave à l'action de la C.N.I.L. punie d'un an d'emprisonnement et 100 000 F d'amende.

Le Code Pénal comporte sept infractions de nature délictuelle – antérieurement prévues aux articles 41 à 44 de la loi de 1978 – énumérées dans la section V du chapitre VI du titre II du livre deuxième, aux articles 226-17 à 226-22, soit la mise en œuvre d'un traitement sans formalité préalable (création d'un fichier clandestin), punie de 3 ans d'emprisonnement et 300 000 F d'amende, le non respect de l'obligation générale de sécurité des informations (5 ans et 2 000 000 F), la collecte d'informations par un moyen frauduleux, déloyal ou illicite, ou malgré l'opposition légitime des personnes (5 ans et 2 000 000 F), la conservation des données au-delà de la durée prévue, sans l'accord de la C.N.I.L. (3 ans et 300 000 F), le détournement de la finalité du traitement (5 ans et 2 000 000 F) et la divulgation des informations à des tiers non autorisés (1 an et 100 000 F).

L'article 226-24 prévoit, par ailleurs, la responsabilité pénale des personnes morales, qui encourent, outre l'amende, la peine d'interdiction d'exercer, le placement sous surveillance judiciaire, la fermeture de l'établissement, l'exclusion des marchés publics, la confiscation et la publicité de la décision.

Enfin, l'article 226-23 étend l'application des articles 226-17 à 226-19 aux fichiers manuels.

Section 4 : LA JURISPRUDENCE

Le Conseil constitutionnel

Le Conseil constitutionnel n'a pas eu à se prononcer sur la conformité de la loi du 6 janvier 1978 à la Constitution mais il a, par deux fois, reconnu que certaines de ses dispositions protégeaient la liberté individuelle. Sont, en conséquence, conformes à la Constitution les lois qui créent un traitement automatisé de données nominatives dès lors que : " le législateur n'a pas entendu déroger aux dispositions protectrices de la liberté individuelle prévues par la législation relative à l'informatique, aux fichiers et aux libertés " (DC 92- 316, 20 janvier 1993, *Loi relative à prévention de la corruption et transparence de la vie économique*) ou bien encore lorsque : " le législateur a explicitement entendu assurer l'application " de ces dispositions (DC 93-325, 13 août 1993, *Loi relative à la maîtrise de l'immigration*).

En dépit de plusieurs saisines en ce sens, le Conseil a donc refusé de tirer de la loi du 6 janvier un principe fondamental reconnu par les lois de la République du respect de la vie privée et de la stricte confidentialité des données nominatives informatisées. Cela ne signifie cependant pas que le Conseil ignore le droit au respect de la vie privée dont il fait une composante de la liberté individuelle laquelle, a-t-il rappelé, figure – avec la liberté d'aller et venir et l'inviolabilité du domicile – au nombre des " libertés publiques constitutionnellement garanties " (DC 94-352, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*). De sorte qu'en définitive, le Conseil admet que " la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle " (*Ibid.*), ou encore, que " les méconnaissances graves du droit au respect de l [a] vie privée sont (_) de nature à porter atteinte à la liberté individuelle " (DC 97-389, 22 avril 1997, *Loi portant diverses dispositions relatives à l'immigration*).

Ainsi le Conseil reconnaît-il une protection constitutionnelle du droit à la vie privée par le rattachement de ce droit à la liberté individuelle dont relèvent les dispositions de la loi du 6 janvier 1978.

Le Conseil d'Etat

Les arrêts de principe du Conseil d'Etat sur à l'application de la loi du 6 janvier 1978 sont relativement peu nombreux. Ceux-ci concernent en premier lieu et dans une très large mesure les pouvoirs de la CNIL elle-même, étant donné d'une part, l'ambiguïté du régime de déclaration préalable prévu à l'article 16 de la loi ; d'autre part, l'incertitude quant à la portée des avis prévus à l'article 15 ; enfin, l'indétermination juridique s'attachant à certains actes de la CNIL. Les arrêts concernent, en second lieu, les traitements mis en œuvre par le pouvoir réglementaire ou par les personnes privées, qui ont fourni au Conseil d'Etat l'occasion de se prononcer sur les droits des personnes fichées.

Les pouvoirs de la CNIL

En effet, bien que l'administration ne puisse s'en écarter que par règlement pris sur avis conforme du Conseil d'Etat, ce dernier a rappelé que les avis de la CNIL avaient une portée strictement consultative, et n'étaient ni des avis conformes ni des décisions (v. Conseil d'Etat, 26 juillet 1996, *Association des utilisateurs de données publiques économiques et sociales et autres*, CE, 19 mars 1997, *SMEREP*).

Toutefois, puisqu'elle doit, conformément à la loi, donner un avis motivé pour les traitements publics dont la création revient au pouvoir réglementaire, la CNIL a été conduite à assortir ses avis de réserves. La question s'est alors posée de la liberté dont jouissait l'administration à leur égard. En effet, si l'on considérait qu'elle devait reprendre intégralement les réserves de la CNIL dans le texte créant un traitement, l'avis de la CNIL devenait conforme. À l'inverse, si les administrations pouvaient ne pas tenir compte des réserves, l'obligation de recourir à l'avis conforme du Conseil d'Etat pour s'écarter d'un avis de la CNIL perdait de sa portée.

Le Conseil d'Etat n'a pas remis en cause la possibilité pour la CNIL d'assortir ses avis de réserves : tout en maintenant sa jurisprudence sur le caractère consultatif des avis de l'article 15, il a considéré qu'il n'était possible de passer outre aux réserves dont ils sont parfois assortis que par décret pris sur avis conforme du Conseil d'Etat. Ainsi, un avis assorti de réserves n'équivaut pas à un avis favorable. L'administration doit alors en appeler à un tiers : le Conseil d'Etat ou le Parlement lui-même. Cette solution maintient la distinction entre les avis tels que les prévoit l'article 15 de la loi et ceux de l'article 31 al. 2 lesquels sont explicitement qualifiés de conformes.

À la différence des traitements de l'administration, les traitements mis en œuvre par des personnes privées relèvent de la procédure de la déclaration prévue à l'article 16 de la loi. La question s'est posée de savoir si la CNIL était en situation de compétence liée pour accuser réception de ces déclarations ou si, au contraire, elle disposait d'un pouvoir discrétionnaire pour la délivrance du récépissé faisant suite à une déclaration.

Les premiers commentateurs de la loi de 1978 avaient considéré que la CNIL était là en situation de compétence liée : dès lors que la déclaration préalable était effectuée et que l'engagement était pris de conformer le traitement aux exigences de la loi, la CNIL devait délivrer le récépissé.

Cependant, la CNIL a, de son côté, adopté un règlement intérieur quelque peu ambigu : l'article 32 de ce règlement précise que le récépissé est délivré à l'issue de la " *procédure de validation du dossier* " – procédure qui n'est pas prévue par la loi. Le Conseil d'Etat a *annulé le refus* de délivrance du récépissé en considérant que la CNIL ne peut le refuser dès lors que le dossier présenté comporte l'engagement prévu à l'article 16 et est conforme aux prescriptions de l'article 19. Son rôle se borne à " *s'assurer de la régularité* de la déclaration effectuée auprès d'elle au regard des prescriptions des articles 16 et 19 " (Conseil d'Etat, Sect., 6 janvier 1997, *Caisse*

d'épargne Rhône Alpes Lyon).

Le Conseil d'Etat n'a que très récemment posé le critère permettant d'identifier les délibérations de la CNIL faisant grief, retenant celui de l'*interprétation qui ajoute à l'ordonnancement juridique* (Conseil d'Etat, Sect., 9 juillet 1997, *Chambre Synd. Syntec Conseil*). Fait ainsi grief, la délibération qui contient une *décision individuelle de refus* de communiquer l'intégralité d'un compte-rendu d'une mission de contrôle effectuée par la CNIL (Conseil d'Etat, 8 octobre 1993, *Hudin*), d'une décision par laquelle la CNIL *refuse de donner suite* à une plainte (Conseil d'Etat, 28 mars 1997, *Solana*) ; d'une *injonction* de faire droit aux demandes formulées par des clients et tendant à l'accès aux informations contenues dans certains fichiers (Conseil d'Etat, 7 juin 1995, *Caisse régionale de Crédit Agricole de la Dordogne et Caisse nationale de Crédit Agricole*), un *avertissement* adressé au responsable du traitement (CE, 30 juillet 1997, *Sté Consodata*).

Enfin, le Conseil n'a annulé qu'une seule délibération de la CNIL édictant une norme simplifiée (au motif qu'un article de la norme se rapprochait de l'article 31 de la loi, CE, Ass., 12 mars 1982, *CGT*).

Le contrôle des règlements portant création de traitements

Le Conseil d'Etat a également eu à se prononcer sur certains traitements publics autorisés par décret. En revanche, les traitements qui relèvent de la loi échappent à son contrôle, ce que prévoit l'article 15 (Conseil d'Etat, 13 septembre 1995, *Association " Collectif pour la défense du droit et des libertés "*).

Comme on l'a vu, qu'ils soient favorables ou défavorables, les avis prévus à l'article 15 ne font pas grief et ne peuvent donc faire l'objet d'un recours pour excès de pouvoir. Seuls peuvent être contestés les actes réglementaires mettant en œuvre le traitement et pris après avis favorable de la CNIL. Le Conseil d'Etat a exercé à l'encontre de ces règlements un contrôle normal, y compris pour ceux autorisant les traitements prévus à l'article 31 al. 3 qui font exception à l'interdiction posée par l'article 31 al. 1 concernant les données dites sensibles. À cet égard, on doit noter que le Conseil a accepté de contrôler la conformité d'un décret au regard de la Convention du Conseil de l'Europe signée à Strasbourg le 28 janvier 1981 (Conseil d'Etat, 18 novembre 1992, *LICRA et autres*), puis reconnu la compatibilité de la loi du 6 janvier avec cette Convention (CE, 28 juillet 1995, *CGT* (recours contre le décret no 91-1051)). La prise en considération de la Convention a conduit le Conseil à apprécier la proportionnalité d'un traitement nécessaire à l'intérêt public eu égard aux atteintes portées au respect de la vie privée (Conseil d'Etat, 28 juillet 1995, *CGT* (recours contre le décret no 91-1052)) et a jugé qu'est illégal le traitement qui fait indirectement apparaître les opinions religieuses des personnes intéressées, sans que ces dernières aient pu donner leur consentement à ce traitement et sans que les nécessités de l'ordre public n'en justifient l'existence, (Conseil d'Etat, 5 juin 1987, *Kaberseli*).

Les droits des " personnes fichées "

La loi du 6 janvier crée certains droits au profit des personnes fichées, droits que le Conseil semble entendre strictement.

Ainsi, à un requérant qui demandait le retrait d'un fichier de certaines informations le concernant en invoquant leur caractère inexact et équivoque, le Conseil a répondu qu'" en admettant que lesdites informations présentent un tel caractère, il résulte des termes mêmes de l'article 36 de la loi de 1978 que ces informations ne devaient pas être effacées mais rectifiées et clarifiées " (CE, 30 novembre 1994, *Benhaim*). En prenant soin de préciser que cela " résulte des termes mêmes de l'article 36 de la loi ", le Conseil souligne la correspondance que cet article établit entre la qualité des informations contenues et les droits dont dispose la personne concernée. Dans ces

conditions, l'effacement des données doit, selon le Conseil, n'intervenir que si leur collecte, leur utilisation, leur communication ou leur conservation est interdite, tandis que l'inexactitude implique la rectification et l'équivocité, la clarification ; l'incomplétude, le complément et la péremption, la mise à jour.

Par ailleurs, le droit d'accès, qu'il soit direct ou indirect ne permet pas de satisfaire tous les espoirs que certains requérants – lesquels ne peuvent être que des personnes physiques (CE, 15 février 1991, *Eglise de scientologie de Paris*) – placent en lui.

Cela tient d'abord au fait que, comme le précise le Conseil, aucune disposition de la loi ne donne compétence à la CNIL pour ordonner la communication, aux personnes intéressées, des informations les concernant mais que l'obligation de permettre l'exercice du droit d'accès incombe aux personnes qui mettent en œuvre les traitements automatisés, la CNIL n'étant tenue que de faciliter l'exercice de ce droit en intervenant auprès des détenteurs du fichier et, éventuellement, en saisissant le parquet (CE, 17 janvier 1986, *Le Bihan*).

Cela tient ensuite au fait que le Conseil d'Etat se trouve, de par la loi, dans l'impossibilité d'exercer un contrôle de fond sur le caractère suffisant ou non de l'information communiquée. Aussi, à un requérant qui estime que les informations qu'on lui a transmises sont des plus sommaires, le Conseil ne peut-il qu'opposer la consultation effectuée par la CNIL et conclure que ce requérant " doit être regardé comme ayant reçu communication de l'intégralité des informations le concernant " (Conseil d'Etat, 15 décembre 1995, *Bockstal*).

Par ailleurs, le mécanisme de droit d'accès indirect prévu à l'article 39 suppose que le ministre, directement saisi d'une demande d'information, réponde non à la personne dont émane la demande mais à la CNIL elle-même. Est donc conforme à la loi la décision par laquelle le ministre de l'intérieur refuse de communiquer directement à la personne concernée les informations nominatives la concernant lorsque celles-ci sont contenues dans le fichier central de la direction des renseignements généraux (CE, Ass., 19 mai 1983, *Bertin*, CE, 30 novembre 1984, *Bertin* et CE, 27 avril 1988, *Loschak*).

Enfin, le Conseil a précisé les modalités d'exercice du droit d'opposition de l'article 26 notamment en cas de cession de données nominatives à des tiers (CE, 30 juillet 1997, *Sté Consodata*).

La jurisprudence des juridictions judiciaires

La jurisprudence judiciaire a précisé le champ d'application de la loi aux traitements non automatisés, déterminé par la notion de fichier. La jurisprudence a, dans un premier temps, estimé qu'un ensemble de dossiers papiers ne constituait pas un fichier et que les notions de dossier et de fichier s'excluaient l'une l'autre (TGI de Nantes, 16 décembre 1985, CA Rennes, 24 juin 1986, Cass. Crim., 3 novembre 1987).

Les magistrats semblent cependant être revenus sur cette conception qu'avaient critiquée la CNIL et la doctrine. Ainsi, à propos d'un litige relatif à un dossier de recrutement contenant une analyse graphologique, le Tribunal de grande instance de Paris a d'abord constaté qu'" il ne peut qu'être relevé que le dossier personnel d'embauche de la partie civile où s'est trouvée classée l'étude graphologique litigieuse, ne constitue pas un fichier au sens de la loi précitée ", puis ajouté : " étant observé, en toute hypothèse, qu'il n'est pas démontré, en l'état des explications du prévenu, non démontrées par d'autres éléments de la cause, que ce dossier ait été ensuite conservé par l'employeur dans un quelconque fichier " (TGI Paris, 2 mars 1989, *Min. Publ. et Baron c. Gafner et Fonds national d'assurance formation de l'industrie hôtelière*). Une interprétation *a contrario* de ce jugement permet de conclure que lorsqu'un dossier est conservé

dans un fichier de dossiers, la notion de fichier l'emporte : le dossier est assimilé à une fiche et les données nominatives qu'il contient tombent sous le coup de la loi du 6 janvier 1978.

En ce qui concerne les traitements automatisés, la Cour de Cassation a eu à voir, principalement, de litiges nés de traitements des incidents de paiements ou de débiteurs à poursuivre ce qui explique que cette jurisprudence émane de la Chambre criminelle. Là encore elle se caractérise par sa rareté, laquelle n'a pas empêché une divergence d'appréciation relative à l'interprétation de l'article 26 de la loi et une relative incertitude quant aux modalités d'application du droit d'opposition.

Un litige était né de ce qu'une personne se trouvait inscrite dans un fichier informatisé des incidents de paiements établi à partir d'informations recueillies auprès de tiers. Les premiers juges ont relaxé le responsable du traitement poursuivi pour violation de l'article 26 de la loi réprimée par l'article 226-18 du nouveau code pénal. La Cour d'appel de Paris a condamné le responsable du traitement au motif que la mise en œuvre par la personne physique concernée du droit d'opposition qui lui est reconnu par l'article 26 suppose que celle-ci soit avisée, préalablement à son inscription sur un fichier, de ce que des informations nominatives la concernant sont susceptibles de faire l'objet d'un traitement. La Chambre criminelle n'a pas retenu cette interprétation et cassé l'arrêt d'appel en considérant que " 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 concernée " (Cass. Crim., 25 octobre 1995, *Bernard R. et GIE*). Cette dernière décision s'explique certes par le fait que le nouveau code pénal ne sanctionne que le traitement effectué malgré l'opposition de la personne. C'est donc à cette dernière qu'il incombe de se renseigner, auprès de la CNIL pour les traitements privés, en combinant les articles 34 et 22 de la loi et ce que l'on a qualifié de " droit à la curiosité " se révèle en fait être une obligation de renseignement. La question implicitement soulevée par la Cour d'appel conserve néanmoins une certaine pertinence lorsqu'on tient compte du nombre de traitements qui devraient être déclarés à la CNIL mais ne le sont pas, contrairement d'ailleurs à ce qu'a rappelé la Cour de cassation elle-même (Cass. Crim., 3 novembre 1987).

La Chambre criminelle fait cependant une appréciation souple du champ des personnes concernées par la protection, considérant que " les personnes auxquelles la loi du 6 janvier 1978 accorde protection s'entendent non seulement des personnes faisant personnellement l'objet du traitement d'informations nominatives mais encore de toutes celles qui peuvent être directement ou indirectement concernés par l'exploitation de ce traitement " (Cass. Crim., 19 décembre 1995, *M. R et CPII*). En conséquence, la collecte mais aussi l'enregistrement et la conservation de données suppose – comme l'indique l'article 29 de la loi – une extrême vigilance de la part du responsable du fichier lequel doit, par exemple, éviter les homonymies. Ainsi, toutes les personnes inscrites dans un fichier finissent par avoir connaissance de leur inscription et pourront donc à terme jouir de leur droit d'opposition ou de rectification.

Rare, le contentieux relatif à l'application de la loi du 6 janvier 1978 a donné lieu à des solutions nuancées dont on peut affirmer qu'elles parviennent à concilier la protection de la vie privée ou, plus largement de la liberté individuelle, et la prévention d'atteintes à l'ordre public, dont le Conseil constitutionnel fait un objectif de valeur constitutionnelle. Cette jurisprudence a également contribué à faire émerger, en négatif pourrait-on dire, un autre principe : celui de la liberté de constituer des traitements automatisés dans le respect des limites posées par la loi.

Section 5 : LES INSTRUMENTS INTERNATIONAUX

La Convention du Conseil de l'Europe

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981 (convention no 108), entrée en vigueur le 1er octobre 1985, vise à concilier le respect de la vie privée et la libre circulation de l'information. Elle correspond à la première vague d'adoption de lois de protection des données en Europe (Suède, Danemark, France, Allemagne, Luxembourg) et s'inscrit dans une perspective de protection des droits de l'homme et des libertés fondamentales. Elle garantit, sur le territoire de chaque partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, " le respect dans ses droits et libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant " (art. 1er). Les États membres peuvent en étendre l'application aux données relatives à des personnes morales, ainsi qu'aux fichiers manuels. Ils peuvent aussi déclarer qu'ils n'appliquent pas la convention à certaines catégories de fichiers (non assujetties à une législation en matière de protection des données).

La convention s'applique au secteur public comme au secteur privé. Elle pose les principes de qualité et de sécurité des données et définit les garanties de la personne concernée.

Les données doivent être obtenues et traitées loyalement et licitement, sont soumises au principe de finalité, doivent être adéquates, pertinentes et non excessives, exactes et mises à jour, conservées pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. La collecte des données sensibles, y compris celle des données relatives à la santé et à la vie sexuelle, est interdite à moins que le droit interne ne prévoie des garanties appropriées.

Les droits de la personne concernée incluent le droit de connaître l'existence d'un fichier, d'obtenir, à intervalles raisonnables, la connaissance de l'existence de données la concernant, d'obtenir leur rectification ou leur effacement, et de disposer d'un droit de recours.

Les États peuvent cependant déroger à ces principes, lorsqu'une telle dérogation constitue un mesure nécessaire, dans une société démocratique :

–à la protection de l'État, à la sureté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

–à la protection de la personne concernée et des droits et libertés d'autrui.

La convention introduit également la possibilité d'apporter des aménagements pour les fichiers utilisés à des fins statistiques ou de recherches scientifiques, lorsqu'il n'y a manifestement pas de risque d'atteinte à la vie privée.

Aucune disposition n'évoque l'établissement d'une autorité de contrôle, la convention se bornant à prévoir que chaque partie établit les sanctions et recours appropriés.

Le flux transfrontières entre les parties ne peuvent être interdits ni soumis à autorisation. La convention introduit, lorsque certaines catégories de données font l'objet d'une législation spécifique, la notion de garantie équivalente (*equivalent protection*).

Enfin, la convention met en place un comité consultatif chargé de faire des propositions en vue de faciliter et d'améliorer l'application de la convention.

L'intégration de cette convention dans le droit français a été reconnue à plusieurs reprises par le Conseil d'État.

Dans la décision *LICRA* du 18 novembre 1992, le Conseil d'État était saisi d'un recours contre le décret du 2 février 1990 portant application aux juridictions, pour l'exercice de leurs missions, de l'article 31, alinéa 3 de la loi du 6 janvier 1978 (exception à l'interdiction du traitement des données sensibles, par décret pris en Conseil d'État, sur avis conforme de la CNIL). Il a estimé

qu'il résulte de l'ensemble des dispositions de la loi du 6 janvier 1978 que le droit interne français prévoit les " garanties appropriées " visées par la convention.

Dans la décision *CGT* du 28 juillet 1995, le Conseil d'État, saisi d'un recours dirigé contre le décret du 14 octobre 1991 relatif aux fichiers des renseignements généraux, a été amené à se prononcer notamment sur la légalité du droit d'accès indirect au regard de la convention du Conseil de l'Europe. Faisant application de la jurisprudence *Nicolo* du 20 octobre 1989, le Conseil d'État estime que le requérant met en réalité en cause la compatibilité de l'article 39 de la loi du 6 janvier 1978 avec la convention. Il considère cependant, " eu égard au caractère des traitements concernés ", que " les modalités prévues par ces dispositions ne sont pas incompatibles avec les droits d'accès et de rectification énoncés dans les stipulations conventionnelles ".

Cette convention a été suivie de l'adoption d'une dizaine de recommandations sectorielles du Comité des ministres parmi lesquelles :

–la recommandation no R (81) 1 du 23 janvier 1981 relative à la réglementation applicable aux banques de données médicales automatisées ;

–la recommandation no R (85) 20 du 25 octobre 1985 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct ;

–la recommandation no R (86) 1 du 23 janvier 1986 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale ;

–la recommandation no R (87) 15 du 17 septembre 1987 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police ;

–la recommandation no R (89) 2 du 18 janvier 1989 sur la protection de données à caractère personnel utilisées à des fins d'emploi ;

–la recommandation no R (90) 19 du 13 septembre 1990 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes ;

–la recommandation no R (91) 10 du 9 septembre 1991 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics ;

–la recommandation no R (95) 4 du 7 février 1995 sur la protection des données personnelles dans le secteur des télécommunications, avec une référence particulière aux services de téléphone.

Les Accords de Schengen

L'accord de Schengen du 14 juin 1985 visant à supprimer les contrôles aux frontières communes des États parties prévoit le renforcement de la coopération entre les autorités douanières et de police dans la lutte contre la criminalité, en particulier le trafic illicite de stupéfiants et d'armes, l'entrée et le séjour irrégulier de personnes, ainsi que contre la fraude fiscale et douanière et la contrebande. A cette fin, et dans le respect de leurs législations réciproques, les parties s'efforcent d'améliorer et de renforcer l'échange d'informations, notamment dans la lutte contre la criminalité (article 9).

C'est l'objet du titre IV de la convention d'application du 19 juin 1990 créant le système d'information Schengen (SIS). Les articles 102 et suivants fixent les règles relatives à la protection des données à caractère personnel applicables à ce système. Les données intégrées dans le système Schengen et l'exercice du droit d'accès et de rectification sont régis par le droit

national. Chaque partie désigne une autorité de contrôle chargée dans le respect de ce droit, d'exercer un contrôle indépendant du fichier de la partie nationale du SIS et de vérifier que le traitement et l'utilisation des données intégrées dans le SIS ne sont pas attentatoires aux droits de la personne concernée (article 114). Toute personne a le droit de demander aux autorités de contrôle de vérifier les données le concernant et leur utilisation.

En outre, une autorité de contrôle commune composée de deux représentants de chaque autorité nationale est chargée du contrôle de la fonction de support technique du SIS. Ce contrôle est exercé conformément aux dispositions de la convention d'application du 19 juin 1990, de la convention no 108 du Conseil de l'Europe, en tenant compte de la recommandation R (87) 15 du 17 septembre 1987 relative au secteur de la police, conformément au droit national de l'État.

Les Lignes directrices de l'OCDE

Le document de base de l'OCDE est constitué par les " lignes directrices régissant la protection de la vie privée et les flux transfrontières des données à caractère personnel ". Ce document, qui n'a pas valeur contraignante, a fait l'objet d'une recommandation adoptée le 23 septembre 1980.

Les lignes directrices de l'OCDE sont fondées sur une approche qui privilégie la libre circulation des données de caractère personnel à travers les frontières et la crainte que la disparité entre les législations nationales, en restreignant les flux transfrontières de données, n'entraînent de graves perturbations dans d'importants secteurs de l'économie, en particulier de la banque et des assurances. L'harmonisation préconisée des législations est donc fondée sur la nécessité d'empêcher que les flux internationaux de données ne subissent des interruptions, " tout en contribuant au maintien des droits de l'homme ".

Les lignes directrices traduisent l'expression d'un consensus sur " des principes fondamentaux qui peuvent être intégrés à la législation nationale en vigueur ou servir de base à une législation dans les pays qui n'en sont pas dotés ". Elles se présentent comme des normes minimales susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et la liberté individuelle. Des exceptions (réduites au minimum et portées à la connaissance du public) peuvent cependant être apportées, en particulier au nom de la souveraineté nationale, de la sécurité nationale et de l'ordre public.

Leur champ d'application est largement défini mais laisse une marge d'appréciation aux États. Il s'étend aux données à caractère personnel, dans les secteurs public et privé, qui " compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles ".

Les obligations à la charge des États sont de deux ordres : obligation de protection de la vie privée et des libertés individuelles, et obligation d'assurer la libre circulation des données.

Concernant la protection de la vie privée et des libertés individuelles, les obligations des États portent sur la collecte et la qualité des données, le respect des principes de finalité, de sécurité et de transparence. Les États doivent assurer le droit d'accès et de contestation des intéressés ainsi que la responsabilité du maître du fichier.

Le respect de ces principes par les États membres détermine les obligations relatives à la libre circulation des données et les restrictions légitimes susceptibles d'y être apportées. Les États devraient :

–prendre en considération les conséquences, pour d'autres pays membres, d'un traitement effectué sur leur propre territoire et de la réexpédition des données à caractère personnel ;

–prendre toutes mesures raisonnables et appropriées pour assurer que les flux transfrontières de données à caractère personnel aient lieu sans interruption et en toute sécurité ;

–s'abstenir de limiter les flux de données, sauf lorsqu'un État ne se conforme pas " pour l'essentiel " aux lignes directrices, ou lorsque la réexportation des données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles ;

–éviter d'élaborer des lois, politiques et procédures qui, sous couvert de protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation des données allant " au delà des exigences propres à cette protection ".

Un pays membre peut également apporter des restrictions à l'égard de certaines catégories de données pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays membre ne prévoit pas de protection équivalente.

Pour la mise en œuvre de ces principes à l'échelon national, les lignes directrices laissent une grande latitude aux États. Ceux-ci devraient " établir des procédures juridiques, administratives et autres ou des institutions " à cet effet, et s'efforcer notamment :

–d'adopter une législation nationale appropriée,

–de favoriser et soutenir des systèmes d'autoréglementation,

–de permettre aux personnes physiques de disposer de moyens raisonnables pour exercer leurs droits,

–de prévoir des sanctions et recours appropriés,

–de veiller à l'absence de discrimination.

Enfin, les lignes directrices comportent des obligations d'information et d'assistance mutuelle entre les pays membres. Ceux-ci doivent notamment veiller à ce que les procédures applicables aux flux transfrontières ainsi qu'à la protection de la vie privée soient simples et compatibles avec celles des autres pays membres.

Les Lignes directrices des Nations Unies

Adoptées par l'Assemblée générale des Nations Unies (résolution no 45/95 du 14 décembre 1990), les lignes directrices des Nations Unies établissent les garanties minimum de protection des droits de l'homme qui devraient figurer dans les législations nationales. Bien que dépourvues de valeur juridique obligatoire, elles constituent un texte de référence.

Elles se distinguent des lignes directrices de l'OCDE par la plus grande précision des garanties, notamment en ce qui concerne les données sensibles, l'accent mis sur la protection des droits de la personne ainsi que l'extension de leur champ d'application aux organisations internationales gouvernementales. C'est en outre le premier instrument international à recommander la mise en place d'une autorité de contrôle (à la différence de la convention no 108 du Conseil de l'Europe).

Ces garanties s'appliquent aux fichiers publics et privés. Leur possible extension aux fichiers manuels et aux fichiers sur les personnes morales (en particulier lorsqu'ils comportent des informations sur les personnes physiques) est prévue à titre optionnel.

Les lignes directrices interdisent la collecte et le traitement des données selon des moyens déloyaux, illicites ainsi que leur utilisation à des fins contraires aux principes de la charte des

Nations Unies. Elles établissent les principes d'exactitude, d'adéquation, de finalité des données ainsi que les conditions d'exercice du droit d'accès et de rectification.

Le traitement des données sensibles est interdit, sous réserve d'exceptions interprétées de manière restrictive. Les données sensibles sont largement définies. Ce sont les données susceptibles de donner lieu à des discriminations illicites ou arbitraires, incluant les informations sur les origines raciales ou ethniques, la couleur, la vie sexuelle, les opinions politiques, religieuses, philosophiques ou autres, telles l'appartenance à une association ou à un syndicat. Les données de santé ne sont pas mentionnées.

Les seules exceptions aux règles énoncées ci-dessus sont celles nécessaires à la protection de la sécurité nationale, de l'ordre public, de la santé et de la moralité publiques, ainsi que des droits et libertés des personnes, en particulier de celles qui sont persécutées (" clause humanitaire " visant les fichiers des organisations humanitaires sur les personnes arrêtées ou disparues par exemple) sous réserve des garanties appropriées et du respect des conventions internationales relatives aux Droits de l'homme.

Les États désignent une autorité chargée de contrôler le respect des principes énoncés ci- dessus. Celle-ci doit offrir des garanties d'impartialité et d'indépendance.

Les données doivent circuler librement entre les États lorsque ceux-ci offrent des garanties comparables. Dans le cas contraire, les limites ne doivent pas dépasser ce qui est nécessaire à la protection de la vie privée.

L'OMC

L'article XIV de l'accord du 15 avril 1994 établissant l'Organisation mondiale du commerce dispose : " Sous réserve que ces mesures ne soient pas appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable entre les pays où des conditions similaires existent, soit une restriction déguisée au commerce des services, aucune disposition du présent accord ne sera interprétée comme empêchant l'adoption ou l'application par tout membre de mesures (...) nécessaires pour assurer le respect des lois et règlements qui ne sont pas incompatibles avec les dispositions du présent accord, y compris celles qui se rapportent (....) à la protection de la vie privée des personnes pour ce qui est du traitement et de la discrimination des données personnelles, ainsi qu'à la protection du caractère confidentiel des dossiers et comptes personnels ".

La question se pose de savoir si la faculté ouverte par cette disposition peut être transformée en un dispositif plus contraignant. La protection de la vie privée a été évoquée par la Commission européenne lors de la Conférence de Singapour en décembre 1998. La Commission a demandé l'instauration d'un groupe de travail qui se réunira en juin ou juillet 1998.

L'OIT

La protection des données personnelles des travailleurs a fait l'objet d'un recueil de directives pratiques adopté par le BIT le 7 octobre 1996 ( ). Ce document, qui s'adresse directement aux employeurs, n'a pas de valeur contraignante. Il se présente comme un ensemble d'orientations pour l'élaboration des législations, conventions collectives et mesures pratiques dans les secteurs public et privé.

Visant l'emploi de certaines techniques parmi lesquelles la surveillance électronique, le dépistage génétique, les contrôles antidrogue, il a pour objet la préservation de la dignité des travailleurs, la protection de leur vie privée, la garantie de leur " droit fondamental de décider qui peut utiliser quelles données, à quelles fins et dans quelles conditions ".

Outre le rappel d'un certain nombre de principes généraux, ce document contient des dispositions spécifiques aux relations de travail. Ainsi les traitements automatisés ne devraient pas servir à contrôler le comportement des travailleurs, ni être l'élément exclusif de l'évaluation de leurs résultats, ou entraîner de discrimination illégale dans l'emploi ou la profession.

Certains procédés, comme les détecteurs de mensonges, tests de personnalités, dépistage génétique, dépistage de drogues sont strictement encadrés.

Les travailleurs ne peuvent pas renoncer à leurs droits relatif à la protection de leur vie privée et devraient disposer de droits d'accès et d'information étendus. La collecte des données auprès des tiers devrait faire l'objet d'un consentement explicite du travailleur.

Sont considérées comme données sensibles :

–les données relative à la vie sexuelle,

–les opinions politiques, religieuses ou autres,

–les condamnations pénales.

La collecte des données relatives à l'appartenance ou l'activité syndicale est clairement encadrée ainsi que celles des données médicales. Ces dernières ne devraient être collectées que dans la mesure nécessaire pour :

–déterminer l'aptitude à un poste ;

–satisfaire aux exigences de santé et de sécurité du travail ;

–déterminer les droits et accorder les prestations sociales

Section 6 : BILAN ET PROBLÈMES

En France comme à l'étranger, le système français et son institution centrale, la C.N.I.L., ont une bonne image. C'est ce qui ressort aussi bien de la littérature sur le sujet que de nombreux entretiens avec des représentants du secteur public et privé, d'autres pays, enfin des institutions européennes.

On reconnaît en général que notre autorité de contrôle est réellement indépendante et qu'elle a su veiller avec rigueur au respect des principes posés par la loi de 1978. La qualité de cette loi elle-même, qui fut l'une des premières dans le monde et qui a inspiré dans une large mesure les instruments internationaux – notamment la directive européenne – n'est pas contestée. Un bilan positif de ce droit et de cette activité a été dressé à l'occasion du vingtième anniversaire de la loi. La C.N.I.L. a développé une " jurisprudence " par des avis fortement motivés sur les cas individuels et joué un rôle normatif particulièrement utile par ses recommandations et ses " normes simplifiées ". Elle a exercé une action pédagogique auprès des administrations et des entreprises.

Elle est considérée, pour ces motifs, sur le plan national et international, comme une autorité puissante et prestigieuse.

Le système a pourtant révélé des problèmes et des faiblesses.

1) En premier lieu, il est resté centré sur son objectif initial – les grands ordinateurs publics – et ne s'est pas adapté au passage à la *micro-informatique répartie et multipliée*. On parlait dans les années 1970 d'" ordinateurs universels ", grâce auxquels un Etat-Léviathan aurait su tout sur tous, comme le montrait le film italien *Enquête sur un citoyen au-dessus de tous soupçons*. On

devrait parler aujourd'hui d'" informatique universelle ", car les appareils individuels ont envahi la vie quotidienne, les entreprises, les foyers. Le droit français n'était pas préparé à cette évolution. Il eût fallu l'adapter, même si la directive européenne ne nous y avait pas obligé.

2) En second lieu, notre système a souffert, dans la pratique, d'un *déficit d'effectivité*. Personne n'est en mesure d'évaluer aujourd'hui avec une certaine précision le nombre des traitements automatisés d'informations nominatives, qui constituent l'objet même de la loi. La C.N.I.L. en a enregistré 500 000 environ. Encore ce chiffre doit-il être minoré d'environ 20 %, pour tenir compte des traitements qui ont disparu sans que leur suppression ait été déclarée. De toute façon, le nombre actuel de traitements en fonctionnement est sans commune mesure avec celui des traitements déclarés ou autorisés. Trois millions d'entreprises sont dotés d'un ou plusieurs traitements, parfois plusieurs centaines. Les professions libérales comme les avocats ou les médecins sont en voie d'informatisation rapide – volontaire ou forcée. Les traitements se sont également multipliés dans les administrations publiques – et même là, il en existe encore, et non des moindres, qui n'ont jamais été signalés à la C.N.I.L.. Au total et même en tenant compte des traitements dispensés de déclaration, on peut avancer sans grand risque d'exagération que quelques millions de traitements ont échappé à son contrôle. Ces traitements ne sont sans doute pas " clandestins ", mais ils sont en tout cas " irréguliers ". Le bilan de la répression, administrative et pénale, est également faible – quelques dizaines de sanctions ou de poursuites.

Pourquoi ? La C.N.I.L. elle-même ne peut être évidemment mise en cause, car elle a utilisé au maximum les moyens réduits dont elle disposait. Peut-être faut-il seulement regretter que les efforts de sensibilisation de l'opinion qu'elle a accomplis par ses rapports annuels et des colloques n'aient pas été plus importants. On peut constater que son existence et la loi de 1978 sont encore trop largement ignorées. En tout cas, nous devons tirer de cette expérience l'idée que les moyens de l'autorité de contrôle, quelle qu'elle soit, devront être dans l'avenir considérablement accrus.

Une autre raison de cette ineffectivité relative tient au déséquilibre, inscrit dans la loi elle- même et accentué dans son application, entre le secteur public et le secteur privé. C'est le premier qui a retenu l'attention.

3) Force est de constater, en outre, que de très importants *fichiers de sécurité*, qui concernent tous les citoyens et qui comportent de graves dangers pour leurs droits et leurs libertés ont fonctionné longtemps, et que certains fonctionnent encore, sans autorisation. Le problème est ici différent. La C.N.I.L. a bien été saisie de ces traitements. Mais, à plusieurs reprises, elle n'a pas donné un avis favorable au projet qui lui était présenté. En pareil cas, la procédure prévue par l'article 15 de la loi de 1978 a montré ses limites. Cette disposition permet en effet au gouvernement de passer outre à l'avis défavorable de la C.N.I.L. par un décret pris sur avis conforme du Conseil d'État. Cette procédure n'a pas pu jouer pour plusieurs raisons : les gouvernements hésitent à faire en quelque sorte " appel " de la C.N.I.L. au Conseil d'Etat et à se trouver ainsi enfermés entre deux avis d'autorités qui, dans les deux cas et de façon inhabituelle dans notre droit, le lient ; ils préfèrent continuer à négocier avec la C.N.I.L. pour aboutir à un compromis hypothétique. Elle a en outre l'inconvénient de ne pas permettre au juge de se prononcer ; en effet le Conseil d'Etat a jugé conformément à sa jurisprudence habituelle que des avis négatifs, même s'ils ont pour effet de lier l'autorité compétente, ne constituent pas des décisions susceptibles de recours. Ainsi la procédure se trouve-t-elle bloquée aussi bien à l'égard des administrations qui sont liées qu'à l'égard des tiers qui ne peuvent se pourvoir contre un avis négatif. Nous sommes là dans une situation qui s'apparente à du non droit ; on peut observer que les lois qui autorisent des organismes comme les services de police ou les caisses de sécurité sociale à consulter de tels fichiers n'exigent jamais, comme il serait normal, qu'ils aient été " légalement autorisés ". Une telle situation n'est satisfaisante ni pour les fonctionnaires eux-

mêmes, dont beaucoup ont conscience de ne pas respecter le droit qu'ils ont pourtant pour mission de faire appliquer, ni pour les citoyens.

Ces derniers souffrent également, dans cette matière des fichiers et traitements de sécurité, d'une formule qui ne semble pas avoir donné satisfaction : le " droit d'accès indirect ". On sait en effet que le droit d'accès d'un individu aux informations le concernant est l'une des pièces maîtresses de la loi française, comme, d'ailleurs, de la directive européenne ; c'est une application essentielle du respect de la vie privée et du principe de transparence. Or il ne peut évidemment s'appliquer en matière de sécurité : l'Etat ne saurait permettre à un individu de savoir librement si par hasard il ne serait pas inscrit sur un fichier de grand banditisme, de terrorisme ou de trafic de drogues. C'est pourquoi la loi de 1978 a posé la règle selon laquelle, dans ces cas, l'intéressé s'adresserait à la C.N.I.L. qui exercerait le droit d'accès pour son compte par l'intermédiaire d'un de ses membres ayant la qualité de magistrat. Mais trop souvent les services ne leur montrent que des dossiers partiels, des informations lacunaires, se réduisant parfois à des coupures de presse. Il ne faudrait sans doute pas supprimer cette formule, mais la renforcer.

4) La multiplication des *lois particulières* constitue sans doute une autre faiblesse de notre système.

Non par son existence même. En effet, elle n'est pas spéciale à la France, puisque, selon nos informations, il en existerait en Allemagne plus de 80 au niveau fédéral, auxquelles s'ajoutent les lois des Lander. Mais par les incohérences qui l'ont caractérisée au fil des années : rapports avec la loi générale de 1978, de l'inclusion à l'ignorance ; définition du domaine de la loi ; contenu. Ce n'est pas la loi de transposition qui pourra y remédier, mais les pouvoirs publics devraient se doter d'une doctrine sur ces différents points.

5) Enfin, les *relations internationales* n'ont pas été gérées, dans ce domaine, d'une manière suffisamment efficace et cohérente. Trop d'autorités y participent, selon des modalités diverses : ministères des affaires étrangères, de la justice et de l'industrie ; secrétariat général du gouvernement et secrétariat général du comité interministériel pour les questions économiques européennes ; la C.N.I.L. elle-même. Dans le contexte actuel de mondialisation, et compte tenu de l'intérêt accru porté à ces questions par les grandes organisations internationales – Union européenne, Conseil de l'Europe, OCDE, Nations- Unies – il est indispensable de définir des orientations claires et de mieux répartir les rôles.

Chapitre II

LA DIRECTIVE EUROPEENNE DU 24 OCTOBRE 1995

Section 1 : HISTORIQUE

Dans les années 70 et 80, des lois nationales ou locales ont été votées sur le thème traité en France par la loi de 1978. Sur le même sujet, en 1980, l'OCDE a défini des " lignes directrices " et en 1981, le Conseil de l'Europe a. adopté une Convention. A la fin de la décennie, en 1990, la Communauté européenne a décidé d'entreprendre la rédaction d'une directive.

Il n'était pas évident que cette question relève de la compétence de la Communauté, qui n'avait pas mission de s'occuper de protection des libertés et de la vie privée. La justification de son intervention a été trouvée dans l'idée d'établir seulement la libre circulation des données à caractère personnel, considérées comme des marchandises, tout en sauvegardant la liberté individuelle à laquelle cette circulation pourrait porter atteinte. C'était donc un cas-limite et probablement une première.

Précisément parce qu'il s'agissait d'un problème de liberté, qui mettait en présence des cultures et

des traditions différentes, la négociation a été longue et difficile. Pour les mêmes motifs, le Conseil d'Etat et le Parlement ont rendu des avis explicites et fortement motivés, auxquels il est intéressant de se reporter au moment de la transposition (reproduits en annexe), d'autant plus qu'ils ont revêtu un caractère exceptionnellement solennel. Le Parlement est intervenu en application de l'article 88-4 de la Constitution issu de la révision du 25 juin 1992 et le Conseil d'Etat sur la base de circulaires du Premier ministre de 1992 et 1993 qui exprimaient la volonté du gouvernement de l'associer à la préparation du droit communautaire.

A l'occasion de la proposition de directive sur la protection des données personnelles, le Conseil s'est prononcé en assemblée générale par un avis du 10 juin 1993, (avis publié dans *Les grands avis du Conseil d'Etat*, Paris, 1997, page 399, avec une note de Bernard Stirn). Dans cet avis le Conseil d'Etat a invité le gouvernement à veiller à ce que la directive " ne contienne pas de dispositions qui conduiraient à priver des principes de valeur constitutionnelle de la protection que leur accorde la loi du 6 janvier 1978 actuellement en vigueur ", afin de prévenir " tout risque d'inconstitutionnalité de la future loi assurant la transposition de cette directive ". Après cette position de principe il a énuméré certaines dispositions du projet qui pourraient " conduire à une régression du niveau de protection jusqu'ici accordé à ces principes en droit interne ".

Il est facile de donner satisfaction aux observations du Conseil d'Etat. Les unes ont été suivies d'effets car la directive ne reproduit pas les dispositions contestées. Les autres peuvent être aujourd'hui respectées car il s'agit de dispositions facultatives pour les Etats membres, et qu'il suffit donc de ne pas les reprendre en droit interne. En revanche il est plus difficile d'appliquer la recommandation du Conseil d'Etat qui souhaitait que l'harmonisation des législations nationales soit vraiment réalisée malgré le caractère peu contraignant de la directive. En effet les exceptions, limitations et dérogations qu'elle prévoit laissent aux Etats membres une marge de manœuvre dont la France ne peut évidemment pas contrôler l'usage.

L'Assemblée nationale s'est prononcée peu après par une résolution du 25 juin 1993. Elle a souligné que l'objectif de la Communauté européenne ne pouvait " justifier son intervention dans la réglementation des traitements des données à caractère personnel qu'à la condition que la réalisation de cet objectif ne nuise pas au haut degré de protection dont doivent bénéficier les personnes physiques à l'égard de ces traitements et encore moins à assimiler ces données à de simples marchandises ". L'Assemblée considère que la proposition de directive " permet au législateur français de maintenir, pour l'essentiel, l'effectivité de la protection assurée aux individus par la loi du 6 janvier 1978 ", mais, comme le Conseil d'Etat, elle craint que les options très larges laissées aux Etats membres pour la transposition de la directive ne garantissent pas l'homogénéité de cette protection dans la Communauté européenne.

Elle demande enfin au gouvernement de subordonner son accord à l'obtention de modifications de la proposition de la directive tendant :

" 1) à maintenir intégralement le niveau de protection assuré par la loi du 6 janvier 1978 et l'application qu'en a faite la Commission nationale de l'informatique et des libertés sur des points tels que la définition des critères de licéité des traitements, le délai et la portée de l'examen préalable par l'autorité nationale de contrôle des traitements déclarés, les exceptions à l'interdiction du traitement des données sensibles ;

" 2) à prévenir le risque de divergences dangereuses au moment de la transposition de la directive par les Etats-membres, dans des domaines tels que l'autorisation préalable, les traitements à risques, le droit d'information sur l'existence des traitements et le droit d'accès, la conservation des données pénales, le renforcement des conditions de publicité des traitements faisant l'objet d'une exonération de notification à l'autorité de contrôle ;

" 3) à garantir aux Etats-membres le pouvoir d'interdire le transfert de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat, au besoin par l'instauration d'une procédure d'urgence

permettant à un Etat de s'opposer, en vue de protéger les libertés individuelles aux transferts de telles données " .

Les recommandations de l'Assemblée, comme celles du Conseil d'Etat, ont été suivies lors de la rédaction finale de la directive ou pourront l'être lors de l'élaboration du projet de loi de transposition, sauf quelques exceptions secondaires.

Enfin le Sénat a adopté sur le même sujet une résolution le 7 juin 1994. Il a fait observer que la référence de la directive à des articles du Traité de nature économique, appliquée en l'espèce aux domaines des libertés publiques, conduit à une interprétation extensive des compétences de la communauté, mais que cette intervention est justifiée " s'agissant d'une matière où la protection des libertés publiques se conçoit mieux sur un espace élargi en raison de l'évolution accélérée de la technologie ". Le Sénat souhaitait en conséquence que les Etats membres parviennent " à une harmonisation préalable de leur législation la plus approfondie possible ". Cette condition n'a malheureusement pas été remplie et, faute d'avoir été préalable, l'harmonisation devra résulter autant que possible des transpositions. Ces prises de position ont permis dans une large mesure d'infléchir la directive de manière satisfaisante, comme le montrera l'analyse de son contenu.

Section 2 : CONTENU

La directive no 95-46 du 24 octobre 1995 vise un triple objectif qui peut se résumer en une phrase : harmoniser le droit européen des données personnelles pour faciliter leur circulation tout en protégeant la vie privée et la liberté individuelle. Elle est exceptionnelle, à la fois parce qu'elle porte sur des questions qui touchent directement aux droits de l'homme et parce qu'elle comporte de nombreuses options, exceptions et dérogations, qui laissent aux Etats membres de grandes marges d'appréciation dans sa transposition. Elle pose en principe, dans ses considérants, que le rapprochement des législations nationales " ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit au contraire avoir pour objectif de garantir un niveau élevé de protection dans la Communauté ".

Comme la loi française, après avoir défini son champ d'application, la directive énonce un certain nombre de règles de fond, de procédure et de contrôle. Elle est en outre plus précise sur les flux internationaux de données. Elle crée enfin des institutions européennes spécifiques pour en harmoniser l'application.

Champ d'application

La directive ne s'applique, comme il est normal, qu'aux traitements qui relèvent du champ de compétence de l'Union européenne, c'est-à-dire qu'elle exclut notamment les " traitements de souveraineté " (défense, sécurité publique, sûreté de l'Etat, droit pénal notamment). A cette exception près, elle s'applique dans les mêmes conditions au secteur public et au secteur privé.

Elle s'étend non seulement aux traitements automatisés, mais aussi aux fichiers manuels, en prévoyant pour ces derniers une période transitoire de douze ans.

Elle couvre les sons et les images, à l'exclusion des traitements de vidéosurveillance mis en œuvre à des fins de sécurité publique.

Le droit national applicable est celui du pays d'établissement du responsable du traitement ou, s'il est situé en dehors du territoire de l'Union, celui de l'Etat sur le territoire duquel sont localisés les

moyens mis en œuvre pour le traitement.

Règles

Plus explicites et plus développées que dans la loi de 1978, elles se situent dans la même ligne. Elles concernent essentiellement les obligations des responsables des traitements et les droits des personnes qui en font l'objet.

Les obligations s'appliquent aux données et aux traitements. Les premières doivent être " traitées loyalement et licitement ", " collectées pour des fins déterminées ", " adéquates, pertinentes et non excessives ", " exactes et mises à jour ", conservées pendant une durée limitée.

La licéité de leur traitement est soumise à un certain nombre de conditions alternatives, dont certaines sont subjectives, comme le consentement de l'intéressé, d'autres objectives comme, par exemple, le respect d'une obligation légale, l'exécution d'un contrat ou la mise en œuvre d'une mission de service public.

La collecte et le traitement de données dites " sensibles " – relatives à l'origine raciale et ethnique, aux opinions politiques, aux convictions religieuses et philosophiques, à l'appartenance syndicale, à la santé et à la vie sexuelle – sont en principe interdits, sous réserve d'un certain nombre de dérogations, notamment en matière de santé.

Les responsables ont enfin des obligations de sécurité et de confidentialité.

Les garanties accordées aux personnes concernées comprennent les droits d'être informé, d'accéder aux données, d'en demander la rectification, de s'opposer au traitement, et enfin de ne pas faire l'objet de décisions individuelles automatisées, c'est-à-dire prises " sur le seul fondement d'un traitement automatisé de données destinées à évaluer certains aspects de sa personnalité ".

Des règles particulières concernent d'une part le traitement à des fins statistiques, scientifiques ou historiques, afin de favoriser le développement de la recherche, et d'autre part les médias, afin de protéger la liberté d'expression.

Certaines de ces règles peuvent faire l'objet de limitations et de dérogations dans l'intérêt de la personne, pour la protection des droits et libertés d'autrui ou pour la sauvegarde d'intérêts publics importants.

Ainsi apparaissent les principes fondamentaux, généraux (proportionnalité, sécurité, transparence) ou propres à la matière (finalité, confidentialité), dont la mise en œuvre doit être inscrite dans les lois et règlements de chaque pays et peut être précisée par des codes de conduite sectoriels.

Procédures

Les traitements doivent en principe être notifiés à une autorité de contrôle, avec un certain nombre de renseignements.

Toutefois, ceux qui " sont susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées " doivent être soumis à un examen préalable, qui peut se traduire par un régime d'autorisation. A l'inverse, ceux qui " ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées " peuvent ne donner lieu qu'à une déclaration simplifiée ou même être exonérés de toute formalité – ce qui ne fait pas obstacle, naturellement, à la pleine application des règles de fond.

La définition de ces différentes catégories constitue l'une des principales difficultés de la directive, et peut conduire à de grandes différences, selon l'endroit où les uns et les autres auront placé les curseurs.

Contrôles

La réduction considérable du nombre de traitements soumis à autorisation préalable est compensée par un renforcement du contrôle a posteriori.

La directive prévoit l'institution d'une autorité de contrôle, sans donner aucune indication sur sa composition ; elle prévoit seulement qu'elle doit agir " en toute indépendance ", et qu'elle doit disposer notamment de pouvoirs d'investigation, d'information et de sanction soumis à un contrôle juridictionnel.

Flux internationaux

La directive pose en principe qu'au terme de sa transposition, la protection assurée en matière de données personnelles sera " équivalente " dans les Etats membres de l'Union européenne, et qu'ainsi, il n'y aura plus de raison " de faire obstacle à leur libre circulation entre eux ". En revanche, elle prévoit une réglementation stricte et détaillée des transferts de données vers les " pays tiers ", c'est-à-dire extérieurs à l'Union. Ces transferts ne peuvent être admis que si le pays de destination assure un niveau de protection " adéquat ", qui est évalué conjointement par les Etats membres et par la Commission européenne. Un certain nombre de dérogations sont toutefois prévues, fondées sur des critères objectifs ou sur des " garanties suffisantes " offertes par le responsable du traitement.

Institutions européennes

Pour veiller à l'harmonisation continue des droits des Etats membres, la directive institue deux organismes spécifiques : le " groupe de protection des personnes à l'égard du traitement des données à caractère personnel " composé de représentants des autorités nationales de contrôle et de la Commission, et un " comité ", composé de représentants des Etats et de la Commission.

Section 3 : COMPARAISON AVEC LA LOI DU 6 JANVIER 1978

Des principes communs

L'analyse du droit national et de la directive européenne démontre que l'une et l'autre se fondent sur un corpus de principes communs, que l'on retrouve d'ailleurs dans de nombreuses législations nationales et dans des textes internationaux, comme ceux du Conseil de l'Europe, de l'O.C.D.E. ou des Nations-Unies.

Ces principes concernent les données, les traitements et les personnes.

Les données doivent être exactes et pertinentes ; les données dites " sensibles " doivent être particulièrement protégées ; les traitements sont soumis aux principes de finalité, de sécurité, de proportionnalité et de transparence ; les personnes concernées ont le droit d'être informées, de refuser leur consentement lorsqu'il est prévu, d'accéder à leurs données, d'en demander la rectification et de s'opposer aux traitements. Une autorité indépendante de contrôle doit veiller à l'application de ces règles.

Des différences importantes

En dehors de questions de mise en œuvre et de différences mineures, la comparaison de la loi française et de la directive européenne révèle trois différences principales.

La première tient *à l'égalité de principe entre secteur public et privé*. Pour des raisons historiques déjà rappelées, le législateur de 1978 s'est inquiété surtout des menaces résultant des grands ordinateurs d'Etat, sur lesquels il a concentré son attention, en soumettant les traitements publics à une autorisation alors que les traitements privés donnaient lieu à une simple déclaration.

Désormais, conformément à ce qu'avait déjà décidé la loi du 1er juillet 1994 sur les registres de recherche en matière de santé, les deux secteurs sont mis sur un pied d'égalité, non seulement pour les règles applicables, mais aussi pour les formalités imposées. C'est un incontestable progrès. En effet, il est apparu à l'expérience, surtout avec la diffusion de l'informatique, que les risques générés par le secteur privé sont aussi importants, même si leur nature est en partie différente, que ceux qui découlent du secteur public. Il arrive, au surplus, que des établissements se trouvant dans des situations analogues se répartissent entre les deux secteurs, et il n'est pas normal qu'ils soient soumis à des régimes différents. C'est le cas, par exemple, des écoles publiques et privées, ou encore des hôpitaux publics et des cliniques privées.

Il résulte de cette assimilation l'une des principales difficultés de la transposition, qui concerne la frontière entre autorisations et déclarations, ou pour reprendre le langage de la directive, entre " examens préalables " et " notifications ". Dans notre système actuel, le partage est simple : d'un côté, tous les traitements des services publics, même les plus insignifiants ; de l'autre, tous les traitements privés, même les plus dangereux. Le critère est organique, vertical. Il est remplacé par un critère horizontal, conceptuel : seront soumis à examen préalable les traitements " susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées ". L'on se trouve ici devant une difficulté de définition analogue, mais non identique, à celle qui résulte de l'article 34 de la Constitution, qui réserve à la loi les règles concernant " les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ". C'est d'ailleurs un des points sur lesquels, comme l'avaient observé l'Assemblée nationale et le Conseil d'Etat, les divergences les plus grandes et les plus graves peuvent apparaître entre les Etats membres.

L'assimilation des deux secteurs ne sera d'ailleurs pas totale, puisque les traitements de souveraineté, qui posent évidemment des problèmes spécifiques, ne sont pas couverts par la directive.

La deuxième différence fondamentale consiste en *un glissement d'un contrôle à priori vers un contrôle a posteriori*. Elle est d'ailleurs liée à la première, car il serait évidemment impossible de soumettre à autorisation préalable les millions de traitements du secteur privé.

Le contrôle a posteriori est bien prévu dans la loi de 1978 : réception de " réclamations, pétitions et plaintes ", " mesures de sécurité ", avertissements, dénonciations au parquet, sanctions pénales. Mais ce contrôle a peu joué, pour des raisons diverses, parmi lesquelles figurent au premier rang l'insuffisance des moyens matériels de la C.N.I.L. et de ses pouvoirs juridiques, ainsi qu'une sensibilité limitée des parquets et des tribunaux à cette matière nouvelle et technique.

Ce doit être l'un des points forts de la transposition que d'assurer à la fois la reconversion et le renforcement de la C.N.I.L., afin de lui permettre d'assurer des tâches nouvelles, plus lourdes, dans un champ élargi. C'est d'autant plus important que la réduction du contrôle a priori doit être compensée par le développement du contrôle a posteriori, si l'on veut respecter le principe selon lequel le niveau global de protection doit être maintenu, sinon amélioré.

La troisième différence est moins importante : il s'agit de *l'extension de la protection aux données contenues dans les fichiers manuels*.

On sait qu'à l'origine, le projet qui a abouti à la loi de 1978 ne concernait que les traitements automatisés ; il en reste des traces dans la loi votée, telles que l'article 1er (" *L'informatique* doit être au service de chaque citoyen (...) ") et le titre de l'institution de contrôle (" Commission nationale de *l'informatique* et des libertés "). Mais le Parlement a introduit dans la loi, à l'article 45, les " fichiers non automatisés ou mécanographiques ", en leur déclarant applicables un certain nombre de ses dispositions, et il en a modifié le titre, devenu " loi relative à l'informatique, aux fichiers et aux libertés ".

Désormais, c'est l'ensemble du dispositif qui sera applicable aux " fichiers manuels ", mais les Etats-membres peuvent prévoir qu'ils ne devront être mis en conformité avec certains articles de la directive qu'à l'expiration d'un délai de douze ans à compter de son adoption, c'est-à-dire en octobre 2007.

La directive nous donne ainsi l'occasion de mettre à jour notre droit, de l'adapter aux conditions nouvelles apparues depuis vingt ans, de remédier aux difficultés qui ont surgi dans la pratique, enfin de l'améliorer.

C'est dans cet esprit qu'il convient d'aborder sa transposition.

Section 4 : ETAT D'AVANCEMENT DE LA TRANSPOSITION DANS LES AUTRES ÉTATS MEMBRES

L'état d'avancement de la réflexion et de la procédure législative engagées en vue de la transposition est très variable selon les pays.

Mis à part l'Italie et la Grèce où il n'existait pas de loi générale de protection des données, aucun État membre n'a à ce jour transposé la directive en droit interne.

En Italie et en Grèce, l'absence de loi générale de protection des données avant l'adoption de la directive et le désir de participer au système prévu par les accords de Schengen ont joué un rôle déterminant dans l'adoption rapide d'une législation transposant la directive.

Après quatre ans de discussion au cours desquels ont été examinés plusieurs projets successifs, l'Italie a été le premier État membre à transposer la directive par la loi no 675 du 31 décembre 1996. Celle-ci, complétée par une deuxième loi portant délégation (loi no 676) adoptée le même jour, a été modifiée par deux décrets législatifs (décrets no 123 du 9 mai 1997, et no 255 du 28 juillet 1997) qui apportent un certain nombre d'assouplissements. La Grèce a suivi de peu avec l'adoption de la loi no 2472/97 du 10 avril 1997.

Un projet vient d'être déposé au Parlement en Suède, au Royaume-Uni, aux Pays-Bas et au Portugal (après révision de l'article 35 de la Constitution qui prévoyait une interdiction absolue de traitement des données sensibles). En Finlande également, le projet de loi de transposition devrait être très prochainement soumis au Parlement.

Au Luxembourg, un projet de loi réalisant une transposition partielle de la directive, a été déposé au Parlement au mois d'octobre. Mais c'est seulement à la fin de l'année 1998 qu'une nouvelle loi transposant l'ensemble de la directive sera adoptée.

En Allemagne, un avant-projet a été établi à la fin de l'année 1997 pour être soumis aux 16 *Länder* qui devaient se prononcer d'ici la fin du mois de janvier. Cependant en raison de la nature des divergences qui demeurent et surtout de la difficulté d'engager un débat devant le Parlement à partir du mois de mars, en période de campagne pour les élections générales, la transposition de la directive ne sera vraisemblablement pas réalisée d'ici le mois d'octobre.

Les autres États membres ont engagé, à partir de 1997, la réflexion sur la transposition de la

directive et ont entrepris une concertation en vue de l'élaboration d'un avant-projet de loi.

En Espagne, après révision de la Constitution sur le traitement des données sensibles (comme au Portugal), un avant-projet de loi organique a été établi afin d'être soumis au Parlement à la fin du premier trimestre 1998.

Au Danemark, le ministère de la justice a constitué un groupe de travail regroupant des représentants des différents intérêts (administrations, patronat, syndicats, association danoise des banques) en vue d'établir un rapport et un projet de loi qui devrait être débattu au Parlement au cours du premier semestre 1998.

En Belgique, un projet a été établi et soumis pour avis au Conseil d'État.

En Irlande, une consultation a été engagé par le ministère de la justice, dont les conclusions viennent d'être publiées.

En Autriche, les travaux ont été amorcés à la fin de l'année 1997 au sein du Conseil pour la protection des données. La consultation des partenaires sociaux devrait être engagéee au mois de mars et le projet soumis au Conseil des ministres avant l'été.

Deuxième partie

DE LA DIRECTIVE EUROPEENNE A LA LOI NOUVELLE

Le travail de transposition de la directive a commencé aussitôt après son approbation à la fin de 1995, et devait être achevé trois ans plus tard, le 24 octobre 1998, comme elle le prévoyait. Il était confié au bureau compétent de la direction des affaires civiles et du sceau du ministère de la justice et piloté, selon la procédure habituelle, par le secrétariat du comité interministériel pour les questions de coopération économique européenne. Un rapport, rédigé par deux membres du Conseil d'Etat et remis au Gouvernement à la fin de l'été 1996, devait servir de base à la reprise des travaux. Mais, bien qu'il n'eut pas le caractère d'un document communicable aux tiers, comme étant lié à la préparation d'un projet de loi, il a été connu, attaqué dans certains journaux, publié sur Internet, et il a provoqué des réactions dans l'opinion. Ces débats ont conduit le gouvernement à interrompre provisoirement le processus de transposition, qui n'avait pas repris à la date de la dissolution de l'Assemblée nationale. C'est dans ces conditions que le Premier ministre a demandé la rédaction d'un nouveau rapport, afin de dégager des solutions qui soient non seulement juridiquement correctes, au regard des principes du droit français et de la directive, mais encore, autant que possible, politiquement consensuelles. Avant de les proposer, il convient d'examiner des questions de principe et de méthode.

Chapitre Ier

PRINCIPES ET METHODE DE LA TRANSPOSITION

Cette directive pose à la France des problèmes particulièrement difficiles pour des raisons qui tiennent à son contenu et à la situation particulière de notre pays.

D'une part, elle touche à des questions qui échappent largement à la compétence de l'Union européenne : libertés publiques, sécurité publique, sûreté de l'Etat et défense, droit pénal. Même dans le domaine qu'elle couvre, elle concerne des enjeux culturels et politiques sur lesquels les Etats-membres ont eu beaucoup de peine à se mettre d'accord et ont dû passer un certain nombre de compromis, ce qui explique le grand nombre de dérogations, limitations et exceptions qu'elle prévoit elle-même aux principes qu'elle pose. En d'autres termes, ce n'est pas une directive rigide et contraignante ; elle laisse place à des choix, à des options, de sorte qu'il peut en être fait, sur des points essentiels, plusieurs lectures.

D'autre part, notre pays est l'un des premiers à s'être doté d'une loi importante en ce domaine, qui a été appliquée pendant vingt ans et complétée par une trentaine d'autres textes législatifs, de nombreux actes réglementaires et une convention internationale, la convention 108 du Conseil de l'Europe. La mise en œuvre de cet ensemble de textes a été contrôlée et coordonnée par la Commission nationale de l'informatique et des libertés et a donné lieu à des décisions importantes du Conseil constitutionnel, du Conseil d'Etat et de la Cour de cassation. Il n'est pas possible de faire abstraction de ce corpus juridique au moment d'y introduire la directive européenne, d'autant plus que celle-ci s'est largement inspirée de celui-là, même si elle en diffère sur quelques points importants.

Au delà des péripéties qui ont été rappelées, c'est la raison principale des difficultés de cet exercice. Ce n'est pas par hasard qu'à l'inverse, les deux pays qui ont procédé les premiers à la transposition de la directive, en 1997 – l'Italie et la Grèce, sont les seuls qui n'étaient pas encore dotés d'une législation en la matière.

Section 1 : LE NIVEAU DE PROTECTION

La directive pose en principe, dans son considérant no 10, que sa transposition ne doit pas avoir pour effet d'abaisser le niveau de protection actuellement assuré dans les Etats- membres :
" l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire ; pour cette raison, le *rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent, mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté*. "

Ce principe fondamental doit être l'un des fils conducteurs de la transposition ; certes, il ne figure que dans les considérants de la directive et non dans son texte. Mais on sait qu'en droit communautaire, les considérants ont plus de valeur que, par exemple, les termes de l'exposé des motifs en droit français. Il en résulte une difficulté, pour ne pas dire une contradiction : comment concilier la volonté d'harmonisation qui est à l'origine de la directive avec le maintien d'un niveau de protection qui, en France, était plus élevé que dans d'autres pays européens ? et, plus précisément, comment évaluer le niveau de protection, qui n'est pas aussi facilement quantifiable qu'un niveau de pollution ? faut-il l'apprécier globalement – les " plus " compensant les " moins " – point par point, article par article ?

On peut donner deux exemples de ces difficultés :

–la directive exprime clairement une préférence pour un régime de déclaration des traitements plutôt que pour un régime d'autorisation, et fait prévaloir le contrôle a posteriori sur le contrôle a priori. S'agit-il, pour la France, d'un abaissement du niveau de protection ? Oui, si l'on s'en tient au champ des autorisations qui, en tout cas pour le secteur public, sera beaucoup plus réduit qu'aujourd'hui. Non, si l'on prend en considération que certaines catégories de traitements privés passeront du domaine de la déclaration à celui de l'autorisation et que le renforcement de la répression compensera la réduction des examens préalables ;

–une difficulté du même ordre concerne l'épineuse question des flux transfrontières de données. La loi de 1994 sur la recherche en matière de santé les limite aux pays bénéficiant d'une protection équivalente, alors que la directive fait état d'une " protection adéquate ", expression qui parait moins exigeante. Là encore, une conciliation devra être tentée entre l'harmonisation européenne par la directive et le maintien nécessaire de notre niveau de protection.

C'est d'autant plus nécessaire, et difficile, qu'il convient de tenir compte, outre le principe posé par la directive, de la jurisprudence du Conseil Constitutionnel en matière de libertés. Selon celle-ci, les garanties des libertés, une fois affirmées, ne doivent pas être ensuite diminuées : c'est ce qui est familièrement dénommé " l'effet de cliquet ". Même si la directive l'autorisait, le niveau national de protection de la liberté individuelle ne pourrait être abaissé ; si elle l'imposait, il faudrait peut-être modifier la Constitution, mais il est possible, et souhaitable, de ne pas l'interpréter en ce sens.

En tout état de cause, le niveau de protection dans un pays déterminé ne peut plus – compte tenu des possibilités de transfert d'informations – être apprécié en isolant sa loi nationale : l'amélioration du niveau de protection dans les autres Etats européens aura un effet bénéfique pour les personnes résidant en France, en évitant les délocalisations à l'intérieur de l'Europe.

Section 2 : LES METHODES LEGISLATIVES

La nature et le champ d'application des lois relatives à la protection des données à caractère personnel posent un certain nombre de questions.

Faut-il réunir dans une même loi les traitements qui sont couverts par la directive et ceux qui lui échappent, en vertu de son article 3, parce qu'ils se situent en dehors " du champ d'application du droit communautaire " **?**

En faveur d'une réponse négative, on pourrait faire valoir qu'il serait plus clair de disposer de deux lois : l'une pour les traitements exclus de la directive, qui pourrait reprendre largement le texte actuel, et l'autre pour les traitements qui y sont inclus, qui procèderait à la transposition.

Mais cette solution ne serait simple qu'en apparence et parait devoir être écartée, pour deux motifs.

En premier lieu, la plupart des dispositions seraient nécessairement identiques : par exemple, celles qui concernent les droits fondamentaux des personnes, l'autorité de contrôle ou encore le régime pénal. Il en résulterait soit des répétitions, soit des renvois d'une loi à l'autre.

En second lieu, il vaut mieux confirmer l'unité des règles juridiques dans cette matière et profiter des aspects positifs de la directive pour réformer notre système même dans les cas où nous n'y sommes pas obligés.

La question de l'unité de la loi revêt un autre aspect, qui est plus délicat : **faut-il profiter de la transposition pour " rapatrier " dans la loi générale les textes spécifiques, nombreux et disparates, qui sont intervenus en France depuis 1978** et prévoir, du même coup, d'y intégrer les dispositions analogues qui ne manqueront pas de s'y ajouter **?**

Il serait intéressant de procéder à cette sorte de " codification ", pour la commodité des usagers de cette branche du droit. Ce serait en outre l'occasion d'étendre à ces lois spéciales le contrôle de la loi générale qu'exerce actuellement le ministère de la justice, qui en est le gardien et le garant. Mais ce n'est pas possible.

Certes, la loi de 1994 sur la recherche en matière de santé a bien été incorporée dans la loi de 1978. Mais c'est la seule. Elle a d'ailleurs été présentée au Parlement non par le ministre de la justice, mais par celui de la recherche, et elle a sans doute vocation à être retirée de la loi " informatique et libertés " pour être introduite dans un " code de la recherche ", actuellement en préparation.

D'une façon plus générale, il ne parait pas possible d'interdire aux différents ministres de présenter et de défendre des textes propres aux fichiers et aux traitements de leur département.

En outre, la loi générale deviendrait difficile à lire et à appliquer si elle était encombrée par des dispositions particulières multiples et disparates. Quant aux usagers du droit, ils préfèrent sans doute trouver les textes qui leur sont applicables dans des codes auxquels ils sont habitués, comme les codes de procédure pénale, du travail, de la sécurité sociale ou de la route. Une dernière raison de maintenir une pluralité de textes est fournie par le droit communautaire lui-même, qui est engagé dans la même voie : dès maintenant a été adoptée une directive spécifique sur la protection des données à caractère personnel en matière de télécommunications, dont la transposition doit intervenir dans le même délai que la directive générale.

A défaut d'une unification improbable, voire impossible, il serait du moins souhaitable que ces lois soient harmonisées, au moins dans leurs rapports avec la loi générale de 1978.

Ces textes spécifiques posent une autre question : **quel est, en matière de fichiers et de traitements, le domaine de la loi ?**

Dans l'immédiat, il convient de vérifier, comme pour la loi générale de 1978, si les lois spécifiques doivent être affectées par la transposition de la directive.

On peut mettre dans la catégorie des traitements relevant du domaine de la loi les grands fichiers de police et de sécurité, les traitements qui risquent de porter atteinte à des secrets particulièrement protégés par la loi comme le secret bancaire et le secret médical ou les interconnexions de fichiers sociaux, fiscaux et policiers. " Les règles concernant la procédure pénale " et " les principes fondamentaux de la sécurité sociale " mentionnés par l'article 34 de la Constitution peuvent également fournir des critères de définition du domaine de la loi en matière de protection des données personnelles.

Autre question de politique législative : **faut-il, pour transposer la directive, procéder par modification de la législation actuelle, en particulier de la loi de 1978, ou faut-il rédiger une loi entièrement nouvelle ?**

Plusieurs arguments peuvent être invoqués en faveur de la seconde solution : elle marquerait plus nettement le passage d'un système à un autre ; elle permettrait une présentation plus claire du texte ; elle faciliterait ainsi son examen et la vérification de la qualité de la transposition.

Il nous parait pourtant préférable de procéder par modification des textes en vigueur, pour une raison symbolique et une raison technique. Tout d'abord, la loi de 1978 a été souvent reconnue comme une " bonne loi " ; sans avoir la même importance, elle a un caractère " fondateur ", comme la loi de 1881 sur la presse ou celle de 1905 sur les associations ; elle a été remarquablement préparée, par une série d'études approfondies dont le rapport couramment appelé " rapport Tricot ", du nom de son principal rédacteur ; enfin, ce fut une des premières lois du genre non seulement en Europe mais dans le monde et elle a atteint un prestige international comparable à son autorité nationale ; c'est précisément pour ce motif qu'elle a largement inspiré la directive européenne. Il serait dommage de la faire disparaître à l'occasion de l'introduction de cette dernière dans notre droit national.

Il est vrai que cette solution présente certains inconvénients techniques : la loi de transposition, qui comportera de nombreuses modifications plus ou moins importantes, n'aura pas la présentation plus élégante d'un texte entièrement nouveau ; mais le travail du Parlement pourra être facilité s'il dispose d'une maquette complète de la loi telle qu'elle sera une fois les modifications adoptées. En outre, il est inutile d'alourdir les débats en y incluant des dispositions qui ont fait leurs preuves et dont la directive n'impose pas la révision, et ces dispositions sont nombreuses.

Une dernière question se pose : **faut-il profiter de la transposition de la directive pour**

procéder à des réformes qu'elle n'impose pas ?

Il est vrai que certaines dispositions de la loi de 1978 sont apparues à l'usage, mal adaptées ou difficiles à mettre en œuvre, comme celles de l'art. 15 *sur la procédure d'autorisation des traitements des services publics. La composition de l'autorité de contrôle* peut être réexaminée en fonction de l'expérience et de la modification des ses pouvoirs. *Le dispositif pénal* a manqué d'efficacité.

Une autre réforme aurait pu être envisagée : *l'extension aux personnes morales de la protection des informations nominatives*. Certains pays se proposent de le faire, à l'occasion de la transposition. En France même, le rapport qui est à l'origine de la loi et le projet déposé au Parlement se prononçaient dans le même sens. Mais le législateur a préféré y renoncer, parce que les enjeux sont différents : vie privée et liberté individuelle d'un côté, et secret des affaires de l'autre.

La CNIL elle-même a repris l'idée dans son second rapport annuel ; elle semble y avoir renoncé ensuite, tout en soumettant partiellement à la loi les fichiers " mixtes " qui portent sur des personnes morales tout en comprenant des informations relatives à des personnes physiques, telles que les dirigeants, associés ou actionnaires.

Les entreprises individuelles – artisans, commerçants, professions libérales, entreprises unipersonnelles à responsabilité limitée, même si ces dernières sont juridiquement des personnes morales – doivent également, semble-t-il, être couvertes par la loi, car elles se confondent avec des personnes physiques. Mais ce sera à la pratique et, le cas échéant, à la jurisprudence d'en décider.

De même, les données personnelles concernant les dirigeants et responsables d'entreprises, quelle qu'en soit la forme juridique, sont protégées par la loi de 1978 comme par la directive ; mais c'est la simple application du droit commun, car il ne s'agit pas là de fichiers de personnes morales.

Il arrive également que ces données posent pour les personnes morales des problèmes identiques à ceux des personnes physiques et qu'elles soient soumises au même régime. C'est le cas des abonnés au téléphone dont la protection s'étendra à ceux qui ont la qualité de personnes morales en application de la directive européenne sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, dites " directive télécom ". Cette directive pose toutefois une distinction, car en ce qui concerne des personnes morales, elle ne vise pas des " droits " mais des " intérêts légitimes ".

Quant aux personnes morales proprement dites, au-delà de ces cas particuliers, la question de prévoir pour elles une loi analogue mériterait une réflexion approfondie et ne peut être réglée à l'improviste dans le cadre de la transposition d'une directive consacrée expressément et exclusivement aux personnes physiques.

Section 3. : LES TERRITOIRES D'OUTRE-MER

La loi de transposition doit-elle s'appliquer dans les territoires d'outre-mer ?

Cette question est double :

–la transposition de la directive doit-elle être de plein droit étendue à ces territoires ?

–sinon, est-il opportun de l'étendre ?

Sur le premier point, la réponse est négative. Il s'agit d'une directive dite " marché intérieur ", qui a pu être rattachée à la compétence européenne parce que les données personnelles ont été

considérées comme des marchandises qui doivent, comme telles, circuler à travers le territoire de l'Union. Un tel texte n'est pas, en principe, applicable outre- mer.

Mais, en opportunité, il doit l'être parce qu'il concerne les libertés publiques. La loi du 6 janvier 1978 a été expressément déclarée applicable " à Mayotte et aux territoires d'outre- mer " par son article 47 et une ordonnance du 28 mars 1996 y a ajouté le chapitre V bis, issu de la loi du 1er juillet 1994 sur la recherche en matière de santé, qui en avait été initialement exclu. Ne pas maintenir cette disposition reviendrait, pour ces territoires, à un abaissement de protection, qui, nous l'avons vu, est interdit à la fois par la directive elle- même – et l'on doit tenir compte de cette indication même si elle ne s'y applique pas directement – et par la jurisprudence du Conseil Constitutionnel. Il serait choquant et dangereux que ces territoires ne bénéficient pas, dans un domaine aussi fondamental des libertés, du même régime protecteur que le territoire métropolitain.

Chapitre II

CONTENU DE LA TRANSPOSITION

Articles 1er à 4 : DISPOSITIONS GENERALES

Article 1er : L'objet de la directive

L'article 1er de la directive en définit le double objet : d'une part, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, d'autre part, la garantie de la libre circulation de ces données entre les Etats membres, qui ne peut être restreinte pour des raisons relatives à la protection de ces droits.

Ces dispositions ne paraissent pas appeler de mesure particulière de transposition, dès lors qu'elles trouvent leur pendant dans des règles directement applicables dans l'ordre juridique français.

En effet, l'article 1er de la loi du 6 janvier 1978 comporte un énoncé plus complet de principes protecteurs des droits et libertés des personnes physiques : " 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 aux libertés individuelles ou publiques ".

D'autre part, le principe de libre circulation des données s'impose déjà aux autorités françaises – dans un espace plus vaste que celui de l'Union européenne – en application de la convention du Conseil de l'Europe du 28 janvier 1981, publiée le 20 novembre 1985.

Si elles n'ont pas à être expressément reprises dans la loi du 6 janvier 1978, les dispositions de l'article 1er de la directive posent en revanche les bornes qui doivent guider le processus de transposition : le législateur et les autorités nationales doivent garantir les droits et libertés des personnes physiques, mais les mesures prises à cette fin ne sauraient avoir pour effet de restreindre ou d'interdire la libre circulation des données à caractère personnel entre Etats-membres.

Article 2 : Définitions

L'article 2 de la directive énonce huit définitions : celles des données à caractère personnel, du traitement de données à caractère personnel, du fichier de données à caractère personnel, du responsable du traitement, du sous-traitement, du tiers, du destinataire et du consentement de la personne concernée.

La transposition de la directive impose que les textes français soient strictement mis en adéquation avec ces définitions et donc, dans la plupart des cas, que leurs termes soient repris à la lettre dans la loi du 6 janvier 1978.

Toutes ces définitions ne revêtent cependant pas la même importance : les termes de " données à caractère personnel ", de " traitement " ou de " responsable du traitement " sont les fils conducteurs de la directive ; ils y reviennent en de très nombreuses occurences. En revanche, les notions de " sous-traitement ", de " tiers " et de " destinataire " sont très étroitement liés à l'exercice des droits d'accès et de communication des données.

L'énoncé systématique de définitions en tête d'un texte législatif ou réglementaire correspond à une tradition anglo-saxonne. Il est plus rarement d'usage dans la pratique du législateur français.

Il est proposé, pour rester dans la ligne de cette pratique, de ne reprendre dans le chapitre Ier de la loi du 6 janvier 1978 que les quatre premières définitions énoncées par l'article 2 de la directive : celles des données à caractère personnel, du traitement, du fichier, et du responsable du traitement. Les notions de sous-traitement, de tiers, de destinataire pourront être précisées lors de leur première occurrence dans le texte. La notion de " consentement de la personne concernée " ne semble pas, quant à elle, devoir faire l'objet de définition spécifique, dès lors qu'elle revêt en droit interne la même signification que celle qui lui est donnée dans la directive.

La transposition des définitions énoncées par les points a) à d) de l'article 2 de la directive appelle diverses précisions.

Données à caractère personnel

Les " données à caractère personnel " sont définies par la directive comme " toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs élements spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ".

Cette définition doit se substituer à celle des " données nominatives " – " informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale " – donnée à l'article 4 de la loi du 6 janvier 1978.

Certains commentaires ont souligné que la définition donnée par la directive pourrait donner lieu à une extension du champ de la protection par rapport à la loi de 1978, dans les domaines où la notion d'identification indirecte est source d'incertitudes, comme ceux de la voix et de l'image.

Mais cette extension paraît résulter davantage de la prise en compte des progrès des techniques d'identification (moteurs de recherche, logiciels de reconnaissance vocale ou morphologique) que de l'imprécision de la directive.

La directive s'efforce en effet de poser clairement les critères permettant de délimiter le champ des données concernant une personne identifiable et de les distinguer des données rendues anonymes qui tombent en dehors du champ de la protection. D'une part, l'article 2, a) énumère, à titre d'exemples, une liste d'éléments qui peuvent permettre d'identifier une personne. D'autre part, le considérant 26 énonce précisément les critères qui permettent de déterminer si une personne est identifiable :

–celui des moyens susceptibles d'être raisonnablement mis en œuvre pour parvenir à l'identification de la personne concernée ;

–celui de la personne susceptible de mettre en œuvre ces moyens, qui peut être aussi bien le responsable du traitement lui-même qu'une personne tierce.

Ainsi, le dispositif de vidéosurveillance d'une entreprise entrera-t-il clairement dans le champ de la protection s'il a vocation à permettre l'identification des agents habilités à accéder à certains locaux. De même, les informations codées transmises par un médecin à un laboratoire pharmaceutique sur les réactions des malades à un nouveau médicament constituent des données personnelles, dès lors que le médecin conserve la faculté d'identifier ses patients.

Il est proposé de reprendre littéralement les termes de la définition énoncée par l'article 2, a) de la directive dans la loi du 6 janvier 1978. En effet :

–la notion de " donnée à caractère personnel " paraît en elle-même plus pertinente que celle d'" information nominative ", compte tenu du développement des moyens d'identification indirecte. Elle permet en outre de mettre fin, en droit français, à une confusion entre les " informations nominatives " au sens de la loi du 6 janvier 1978 et les " informations nominatives " au sens de la loi du 17 juillet 1978 qui a pour effet de restreindre la liberté d'accès aux documents administratifs, dès lors que les champs d'application de ce terme dans chacun des deux textes sont distincts ;

–tout décalage entre les termes de deux définitions induirait un risque de contradiction entre la loi et la directive, dès lors que ces définitions délimitent le champ d'application matériel de la protection des données, et que la loi ne saurait modifier l'équilibre entre protection des personnes et libre circulation des données tel qu'il est déterminé par la directive ;

–il ne paraît pas utile de reprendre dans la loi les précisions données par le considérant 26 sur " l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne ". L'autorité chargée de la protection des données et le juge pourront en effet, en tout état de cause, se référer aux motifs de la directive pour éclairer les définitions données par la loi et lever toute difficulté d'interprétation.

Traitement de données à caractère personnel

La notion de " traitement de données à caractère personnel " doit, de la même manière, remplacer celle de " traitement automatisé d'informations nominatives " définie à l'article 5 de la loi du 6 janvier 1978.

Elle recouvre un champ plus vaste que cette dernière notion. En effet :

–la directive vise aussi bien les traitements automatisés que les traitements de fichiers manuels, alors que la loi du 6 janvier 1978 ne soumet ces derniers qu'à des obligations restreintes ;

–la directive s'applique à toutes les formes de traitements automatisés, qu'ils se rapportent ou non à l'exploitation de fichiers ou de bases de données. La Commission a en effet considéré que le concept de fichier – qui est à la base de la plupart des législations nationales – était désormais dépassé dans le contexte du développement de l'automatisation et des télécommunications, et que la seule référence à la notion de traitement devait permettre d'appliquer les règles de la protection à toute technologie et à toute organisation particulière des données ;

–les opérations de collecte des données constituent en elles-mêmes un traitement ;

–la mise en œuvre d'une seule des opérations énoncées par l'article 2, b) de la directive (et non pas nécessairement d'un ensemble d'une chaîne d'opérations) suffit à caractériser le " traitement " des données.

Fichier de données à carctère personnel

Le terme de " fichier de données à caractère personnel " n'est repris qu'aux article 3 et 32 de la directive, pour définir les cas dans lesquels celle-ci s'applique aux traitements non automatisés, et les dispositions transitoires applicables à ces mêmes traitements.

La notion n'est donc pertinente qu'à l'égard des fichiers manuels. Comme on vient de le souligner, la directive régit en effet, en vertu de son article 3.1, précisé par le considérant 15 :

–d'une part, le traitement automatisé de données à caractère personnel, que celles-ci soient contenues ou non dans un fichier ;

–d'autre part, le traitement non automatisé de données contenues ou appelées à figurer dans un fichier.

La notion de fichier recouvre " tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ". Le considérant 15 précise que le fichier ainsi entendu doit être " structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause ".

Certaines des contributions élaborées par les administrations publiques à l'attention de la mission ont souligné qu'il importait de distinguer clairement les fichiers des dossiers non structurés, et de préciser dans la définition du fichier les critères permettant d'établir cette différenciation, en mettant l'accent non seulement sur la structuration interne, mais aussi sur l'accès direct à ces données à partir du nom ou d'un identifiant.

Il semble toutefois préférable de s'en tenir aux termes de la directive. Les précisions suggérées par certaines administrations productrices de fichiers pourraient en effet conduire à réduire le champ de la protection en-deçà de ce que permet la directive.

On observera en effet que les dossiers rassemblant des données à caractère personnel sont rarement – dans l'administration ou dans les entreprises – constitués d'une manière " non structurée " ou qui ne permette pas " un accès aisé aux données à caractère personnel en cause ". Les dossiers sont le plus souvent un mode de classement d'une série de fichiers, selon des critères relatifs aux personnes (ainsi les dossiers de personnel des administrations regroupent-ils les fiches relatives au recrutement, à la carrière et à la notation de chaque agent). En outre, l'accès à ces dossiers peut être " aisé " au sens de la directive sans passer directement par un nom ou un identifiant.

La notion de " dossier non structuré " ne trouvera donc à s'appliquer que dans des cas résiduels et isolés, et semble devoir être exclue lorsqu'est en cause le traitement de séries de données à caractère personnel.

Dans un souci de clarté, et dès lors que la notion de fichier sert exclusivement à délimiter le champ d'application de la directive aux traitements non automatisés, il est proposé d'inverser l'ordre des définitions et de la détermination du champ d'application de la loi, et de les regrouper dans les articles 4 et 5 de la loi :

–l'article 4 reprendrait les termes précités de l'article 3.1 de la directive ;

–l'article 5 énoncerait les définitions des trois termes qui précisent le champ d'application de la loi (données à caractère personnel, traitement, fichier).

Responsable du traitement

La définition du " responsable du traitement " est essentielle – et doit figurer en tête de la loi – dans la mesure où elle détermine la personne physique ou morale sur laquelle les obligations prévues par la directive reposent, et où le lieu d'établissement de cette personne constitue le premier critère de détermination de la loi nationale applicable.

L'article 2, d) de la directive définit le responsable du traitement comme " la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement à caractère personnel ". Le responsable ne doit pas être confondu avec les personnes qui, tels les employés ou les sous-traitants, mettent en œuvre des traitements pour son compte.

La formule employée par la directive pourrait donner lieu à deux interprétations distinctes, selon lesquelles :

–il n'y a qu'un responsable du traitement, qui agit seul ou conjointement avec d'autres personnes,

–ou bien il peut y avoir plusieurs responsables conjoints pour un même traitement.

Il semble que le texte ait été modifié en cours de négociation pour permettre la seconde interprétation. Mais la lettre du texte va plutôt dans le sens de la première, ainsi que les considérations pratiques. En effet, la notion de " responsable " détermine notamment le droit national applicable, et crée une présomption de responsabilité. Or on ne peut imaginer que plusieurs droits nationaux soient applicables en cas de pluralité de responsables, ni que la présomption de responsabilité soit répartie d'office entre plusieurs personnes.

De toutes façons, il suffira dans la loi de transposition de reproduire telle quelle la formule de la directive, et l'autorité de contrôle, ainsi que les tribunaux, apprécieront sa portée.

Le deuxième membre de phrase du point d) prévoit une définition dérogatoire du responsable dans le cas où les finalités du traitement sont fixées par des dispositions législatives ou réglementaires nationales ou communautaires. Cette formule – qui vise sans doute les traitements publics – exclut les dispositions réglementaires prises par les collectivités locales, et la loi française n'a pas, en principe, à se prononcer sur les dispositions communautaires. Mais on peut envisager une formule générale : " sauf s'il en est disposé autrement par une loi ou par un décret, dans leurs domaines respectifs de compétence ".

Article 3 : Champ d'application

L'article 3 de la directive délimite son champ d'application matériel.

Le premier alinéa définit les champs d'applications respectifs de la directive aux traitements automatisés et non automatisés. Pour les raisons exposées ci-dessus, il est proposé d'en reprendre les termes en amont des définitions des données à caractère personnel, des traitements et des fichiers.

Le premier membre du deuxième alinéa exclut du champ d'application de la directive les matières qui ne relèvent pas du droit communautaire – en particulier les activités couvertes par les titres V et VI du traité de l'Union européenne (politique étrangère et de sécurité commune ; justice et affaires intérieures) – et, en tout état de cause, les traitements que l'on peut qualifier de " traitements de souveraineté ", ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal.

Le présent rapport, en définissant les principes et les méthodes de la transposition de la directive, a clairement pris le parti de l'unité des règles juridiques applicables dans les matières communautaires et non communautaires.

Par suite, il est proposé de ne pas reprendre dans la loi du 6 janvier 1978 les dispositions du premier membre du deuxième alinéa de l'article 3 de la directive.

Le principe ainsi posé ne conduit cependant pas à exclure que des lois spéciales – intervenant dans les matières non communautaires ou dans le champ des traitements de souveraineté – puissent déroger aux règles générales énoncées par la loi du 6 janvier 1978 conformément aux objectifs de la directive.

Les principaux régimes législatifs spéciaux sont énumérés en annexe du présent rapport. Tous ne se rattachent cependant pas aux matières situées hors du champ d'application de la directive.

La mission s'est ainsi interrogée sur la conformité à la directive des dispositions de l'article 10 de la loi du 21 janvier 1995, aux termes desquelles " Les enregistrements visuels de vidéeosurveillance ne sont considérés comme des informations nominatives, au sens de la loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés que s'ils sont utilisés pour la constitution d'un fichier nominatif ".

Certes, le considérant 16 de la directive précise que " les traitements de données constituées par des sons et des images, tels que ceux de vidéo-surveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'Etat ou pour l'exercice des activités de l'Etat relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire ".

La difficulté réside dans le fait que le champ d'application de la loi du 21 janvier 1995 paraît plus large que celui des activités visées par les motifs de la directive, dans la mesure où il inclut les dispositifs de vidéosurveillance mis en place par des établissements privés à des fins ne se rattachant pas nécessairement à la sécurité publique, à la sûreté de l'Etat ou à des domaines du droit pénal. La loi autorise en effet les opérations de vidéosurveillance " dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol, aux fins d'y assurer la sécurité des personnes et des biens ". Or, la notion de " sécurité des personnes et des biens ", dans les établissements privés, peut entrer dans le champ d'application de la directive, si elle déborde du cadre strict de la prévention des troubles à l'ordre public et des infractions pénales.

La notion de " sécurité des personnes et des biens " mériterait vraisemblablement d'être précisée. Il conviendrait, en tout état de cause, que les circulaires d'application de la loi indiquent clairement que les dispositifs de vidéosurveillance privés ne sont pas couverts par la loi du 21 janvier 1995 lorsqu'ils sortent du cadre défini par le considérant 16 de la directive.

Le traitement automatisé d'images et de sons enregistrés par des moyens de vidéosurveillance entre en effet dans le champ d'application de la directive – et donc des dispositions générales de la loi du 6 janvier 1978 – dès lors qu'il ne répond pas à l'une des finalités énumérées par les motifs précités, et qu'il permet l'identification des personnes (indépendamment de tout rattachement à la constitution d'un " fichier nominatif " – comme dans le cas des moyens de surveillance mis en œuvre par un établissement à l'égard de ses employés).

Le deuxième membre de l'article 3, alinéa 2, exclut enfin du champ d'application de la directive le traitement de données à caractère personnel " effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques ". Le considérant 12 cite, à cet égard, les exemples de la correspondance et de la tenue de répertoires d'adresses.

Ces dispositions font écho à celles de l'article 45 de la loi du 6 janvier 1978, qui exclut de son champ d'application les fichiers non automatisés ou mécanographiques dont l'usage relève du

strict exercice du droit à la vie privée.

Les termes de la directive doivent, sur ce point, être repris par la loi.

Article 4 : Droit national applicable

L'article 4 de la directive énonce les règles permettant de déterminer le droit national applicable à un traitement donné.

La loi du 6 janvier 1978 ne comporte aucune disposition sur ce point. Or, les règles de détermination de la compétence des autorités nationales sont essentielles à la prévention des conflits de lois, dans un contexte où la facilité des transferts de données multiplie les risques à cet égard.

Le critère principal de détermination du droit national applicable retenu par la directive est celui du territoire dans lequel le responsable du traitement a son établissement. Le traitement doit être " effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre " (article 4, 1, a)). Le considérant 19 précise que " l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable ", et que la forme juridique de l'établissement – qu'il s'agisse d'une simple succursale ou d'une filiale – est indifférente.

Dans le cas où le responsable du traitement dispose de plusieurs établissements situés dans différents Etats membres, le même alinéa (éclairé par le considérant 19) précise que celui- ci doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable aux activités qu'il poursuit. Chaque établissement sera donc soumis à la seule loi de l'Etat sur le territoire duquel il est implanté. Pour reprendre un exemple donné par le *Dictionnaire permanent de droit européen des affaires* (" Protection des données personnelles ", 32), si une entreprise française fabrique au Portugal des produits qu'elle vend en Allemagne à partir d'un établissement situé en France, les traitements de données à caractère personnel impliqués par la gestion du site de production situé au Portugal seront soumis à la loi portugaise, alors que les traitements découlant de la gestion de la clientèle allemande, effectués par l'établissement situé en France, seront soumis à la loi française.

La loi nationale peut également s'appliquer à certains traitements dans le cas où le responsable n'est pas établi sur le territoire de l'Etat membre, en vertu du droit international public. La directive vise, dans l'alinéa b), le traitements de données à caractère personnel effectués par les ambassades et consulats.

Enfin, la directive pose un critère subsidiaire de compétence des lois nationales des Etats membres dans le cas où le responsable du traitement est établi dans un pays tiers, afin de protéger les personnes concernées. Afin d'éviter la délocalisation des établissements responsables dans des " paradis informatiques ", la directive précise que la loi applicable est alors celle du pays dans lequel le responsable " recourt à des fins de traitement de données à caractère personnel à des moyens, automatisés ou non (...) sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la communauté ". Dans ce cas, le responsable du traitement est tenu de désigner un représentant sur le territoire de l'Etat membre, qui remplira notamment ses obligations en matière de déclaration du traitement et d'information des personnes concernées.

Les motifs de la directive ne précisent pas ce qu'il convient d'entendre par " moyens " dans l'alinéa c). Il semble qu'il faille conférer à ce terme l'acception la plus large, et considérer notamment qu'il recouvre tant les moyens en matériel qu'en personnel.

La directive permet ainsi de rattacher à la loi nationale d'un Etat membre le cas où des données à

caractère personnel sont collectées dans cet Etat, par quel que moyen que ce soit, pour être traitées par une entreprise établie dans un pays tiers.

Il est proposé de reprendre ces trois critères dans la loi du 6 janvier 1978, étant entendu – conformément au parti retenu plus haut – que celle-ci doit rester applicable aux territoires d'outre-mer et à la collectivité territoriale de Mayotte.

Il conviendra donc d'inclure dans la loi modificative des dispositions qui la rendront expressément applicables à ces territoires, et de consulter les assemblées territoriales à cet effet.

L'article 5 de la loi pourrait ainsi – après avoir procédé dans un premier alinéa à la définition du " responsable du traitement ", qui conditionne l'application de la loi française – disposer que :

" La présente loi est applicable aux traitements mis en œuvre dans le cadre des activités d'un établissement du responsable sur le territoire de la République française. Doit être regardé comme un établissement l'exercice effectif d'une activité sur le territoire français au moyen d'une installation stable, quelle qu'en soit la forme juridique. Lorsque le responsable du traitement est établi sur le territoire de plusieurs Etats membres de l'Union européenne, les traitements mis en œuvre par ses établissements situés sur le territoire français sont soumis aux dispositions de la présente loi.

" La présente loi est également applicable aux traitements mis en œuvre par les postes diplomatiques et consulaires français.

" Les dispositions de la présente loi s'appliquent enfin lorsque le responsable du traitement n'est pas établi sur le territoire de l'Union européenne et recourt, à des fins de traitement de données à caractère personnel, et notamment pour procéder à la collecte de telles données, à des moyens situés sur le territoire français à des fins de traitement de données à caractère personnel, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de l'Union.

" Dans le cas mentionné au précédent alinéa, le responsable du traitement est tenu de désigner à la commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi, sans préjudice des actions qui pourraient être introduites contre le responsable du traitement lui-même ".

Certains Etats ont été ou envisagent d'aller plus loin dans la définition du champ d'application de leur loi nationale, en y incluant l'ensemble des traitements concernant des personnes établies sur leur territoire. Tel est notamment le sens de la loi grecque et de l'avant-projet de loi luxembourgeois.

L'adoption d'une clause de sauvegarde de ce type permettrait de soumettre à la loi française tout traitement mis en œuvre à partir d'une enquête sur la population française, quel que soit le lieu d'établissement de son responsable ou les moyens mis en œuvre.

Ces dispositions conduiraient cependant à des conflits de lois dans le cas où le responsable du traitement est établi dans un autre Etat membre de l'Union, alors même que la législation de cet Etat garantira aux personnes concernées un niveau de protection équivalent à celui de la loi française. En outre, lorsque le responsable sera établi dans un pays tiers, les dispositions qu'il est proposé d'adopter permettront d'appliquer la loi française en cas de collecte des données en France. Enfin, les dispositions relatives aux transferts de données vers des pays tiers, prises en application des articles 25 et 26 de la directive, garantiront qu'un tel transfert ne sera possible que si le niveau de protection des données personnelles assuré par ce pays est adéquat.

Il ne paraît donc ni utile, compte tenu du niveau de protection garanti, ni conforme aux dispositions de la directive, d'étendre le champ d'application de la loi nationale à l'ensemble des traitements concernant des personnes établies sur le territoire français.

Article 5 : LICEITE DES TRAITEMENTS

L'article 5 de la directive invite les Etats membres à préciser, dans les limites des dispositions du chapitre II (articles 5 à 21), les conditions dans lesquelles les traitements de données à caractère personnel sont licites.

Cet article délimite le cadre général en-deçà et au-delà duquel les dispositions nationales ne peuvent aller. Il n'appelle pas, en lui-même, de mesure particulière de transposition.

Compte tenu de l'ampleur des modifications induites par la directive dans les règles de fond applicables au traitement des données, il conviendra, dans un souci de clarté de la transposition, d'abroger l'essentiel des dispositions du chapitre IV de la loi du 6 janvier 1978 relatif à la collecte, à l'enregistrement et à la conservation des informations, pour les remplacer par un texte entièrement nouveau.

Article 6 : PRINCIPES RELATIFS A LA QUALITE DES DONNEES

L'article 6 contient trois types de dispositions : des principes généraux relatifs à la qualité des données, des prescriptions imposées au responsable du traitement, et enfin des dispositions particulières relatives à la conservation et au traitement des données à des fins historiques, statistiques ou scientifiques.

Principes généraux relatifs à la qualité des données

L'article 6, paragraphe 1, invite les Etats membres à prévoir que les données à caractère personnel doivent être " a) traitées loyalement et licitement ; b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...] ; c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ; d) exactes et si nécessaires mises à jour [...] ".

Cet énoncé de principes généraux relatifs à la qualité des données ne doit pas nécessairement être repris littéralement dans la loi. Il est en effet partiellement redondant avec certaines règles développées dans les articles suivants de la directive.

Ainsi, le point a) ne fait-il que renvoyer d'une part aux conditions générales de licéité des traitements développées dans l'article 7, et d'autre part à l'obligation – édictée par les articles 10 et 11, paragraphe 1 – d'informer les personnes concernées au moment de la collecte ou de la première communication à des tiers (cf. les considérants 38 et 39, qui définissent la notion de " traitement loyal ").

Le point b) pose le principe de finalité, qui constitue une innovation majeure de la directive par rapport à la loi du 6 janvier 1978, mais qui figure déjà presque dans les mêmes termes dans la Convention n 108 du Conseil de l'Europe. La loi de 1978 ne se réfère en effet à la finalité des traitements que de manière incidente, dans les dispositions relatives aux obligations de déclaration.

L'énoncé de ce principe doit être repris dans la loi, dans la mesure où il est une condition de la licéité de la collecte des données (la finalité du traitement doit en effet être déterminée dès le stade de la collecte), et où il pose une exigence de compatibilité entre la finalité de la collecte et celles des traitements ultérieurs. L'adjectif " explicite " est toutefois superflu, dans la mesure où

il renvoie aux obligations d'information de la personne concernée sur les finalités du traitement pour lequel les données sont collectées (article 10, éclairé par le considérant 28) et sur les finalités des traitements ultérieurs à la collecte (article 11, paragraphe 1).

Le point c) dérive de ce principe de finalité une règle de proportionnalité, en précisant que les données doivent être " adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles seront traitées ultérieurement ". Les trois adjectifs employés sont largement synonymes.

Le premier membre du point d) pose enfin un principe d'exactitude des données, qui figure à l'article 37 de la loi du 6 janvier 1978. La directive est toutefois plus explicite que la loi sur l'obligation de mettre à jour les données.

Les principes généraux – de finalité, de proportionnalité et d'exactitude – énoncés par les points b), c) et d) peuvent être regroupés en un seul alinéa, qui disposerait que : " Les données à caractère personnel doivent être collectées pour des finalités déterminées et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Elles doivent être adéquates au regard de ces finalités, exactes et, si nécessaire, mises à jour ".

Prescriptions imposées au responsable du traitement

Le point d) du paragraphe 1, et le paragraphe 2 de l'article 6, dérivent de ces principes généraux des obligations qui pèsent sur le responsable du traitement :

–d'une part l'obligation de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées (art. 6, 1, d) ;

–d'autre part la responsabilité générale du respect des principes énoncés au paragraphe 1 (art. 6, 2).

Ces prescriptions peuvent être reprises dans un alinéa qui disposerait qu'" il incombe au responsable du traitement d'assurer le respect des règles énoncées à l'alinéa précédent, et notamment de prendre toutes les mesures nécessaires pour que soient effacées ou rectifiées les données inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement ".

La référence aux " mesures nécessaires " paraît plus claire en droit français que la notion de " *reasonableness "*, propre au droit anglo-saxon. Il appartiendra à l'autorité de contrôle et au juge de déterminer les circonstances qui permettront d'exonérer le responsable de ses obligations en la matière.

Dispositions particulières relatives à la conservation et au traitement des données à des fins historiques, statistiques ou scientifiques

L'article 6, 1, comporte enfin, dans ses points b) et e), des dispositions qui :

–d'une part, conformément au principe du " droit à l'oubli " posé par l'article 28 de la loi du 6 janvier 1978, prévoient que les données à caractère personnel " doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lequelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement " (alinéa e) ;

–d'autre part, indiquent que le traitement de données " à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible [avec les finalités pour lesquelles les données ont été

collectées], pour autant que les Etats membres prévoient des garanties appropriées ", et invitent les Etats membres à prévoir des garanties pour les données qui sont conservées à de telles fins au-delà de la période prévue à l'alinéa e. Le considérant 29 précise que ces garanties " doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne ".

Le présent rapport se bornera à renvoyer, sur les questions posées par la transposition de ces dispositions, à l'étude précitée du Conseil d'Etat sur *l'Accès des citoyens aux données publiques* : *Pour une meilleure transparence de l'administration*, qui y consacre l'intégralité de son chapitre III.

Le Conseil d'Etat, après avoir relevé les contradictions existant entre la loi du 6 janvier 1978 et la loi du 3 janvier 1979 – la première imposant la destruction des données collectées dans le cadre de traitements automatisés au terme de leur durée d'utilisation courante, sauf autorisation de la CNIL, alors que la seconde subordonne leur élimination au visa de la direction des archives et impose la conservation des documents présentant un intérêt administratif ou historique – propose de distinguer :

–d'une part, la conservation de ces informations, qui doit être autorisée lorsqu'elle se justifie en vue d'un traitement à des fins historiques, statistiques et scientifiques ;

–d'autre part, leur traitement à d'autres fins que les finalités initiales ou celles qui viennent d'être énoncées, qui doit être interdit, sauf dans le cas d'un accord exprès des personnes concernées ou dans l'intérêt de ces personnes et après autorisation de la CNIL.

Article 7 : PRINCIPES RELATIFS

A LA LEGITIMITE DES TRAITEMENTS

L'article 7 pose six conditions alternatives de licéité des traitements, que l'on peut regrouper en trois catégories :

–le consentement de la personne concernée ;

–les conditions procédant d'une nécessité objective : obligation légale ou contractuelle, sauvegarde de l'intérêt vital de la personne ou exécution d'une mission d'intérêt public ;

–en l'absence de consentement et de nécessité objective, les conditions de licéité du traitement sont définies en mettant en balance les intérêts légitimes du responsable du traitement et des tiers auxquels les données sont communiquées avec les droits et libertés fondamantaux des personnes fichées.

Les cinq premières conditions peuvent être transposées presque littéralement, sans difficulté particulière. La loi du 6 janvier 1978 pourra ainsi prévoir qu'" en dehors du cas où la personne concernée a clairement donné son consentement, le traitement de données à caractère personnel ne peut être effectué que s'il est nécessaire à la sauvegarde de la vie de cette personne, à l'exécution d'un contrat auquel elle est partie ou de mesures précontractuelles prises à sa demande, au respect d'une obligation légale du responsable du traitement, ou à l'exécution d'une mission de service public ".

La notion d'" intérêt vital " employée dans la directive est un anglicisme, qui résulte de la traduction littérale des mots " *vital interest* ". Le terme anglais est ambigu, dans la mesure où si, au sens strict, il est synonyme de " question de vie ou de mort ", il peut aussi désigner, de façon plus large, un intérêt essentiel, capital, de première importance, qui ne se rattache pas à la survie de la personne concernée. Il ressort du considérant 31, et des entretiens des membres de la

mission avec les représentants de la Commission, que la directive a entendu utiliser le terme dans son acception la plus stricte. La notion d'intérêt vital vise par exemple la mise en œuvre de traitements de données pour l'identification des personnes victimes de contaminations virales par transfusion sanguine. Afin d'éviter toute confusion à cet égard, il est proposé de retenir les termes de " sauvegarde de la vie de la personne concernée " de préférence à ceux de la directive.

De même, la notion de " mission de service public " – qui figure dans l'actuel article 15 de la loi du 6 janvier 1978 pour délimiter le champ du régime d'autorisation des traitements – est plus claire en droit français que celle de " mission d'intérêt public ou relevant de l'exercice de l'autorité publique " employée par la directive. Le considérant 32 précise, à cet égard, " qu'il appartient aux législations nationales de déterminer si le responsable du traitement investi d'une telle mission doit être une administration publique ou une autre personne soumise au droit public ou au droit privé, telle qu'une association professionnelle ". Conformément à l'esprit de la loi du 6 janvier 1978, la formule générale qu'il est proposé de retenir englobe aussi bien les personnes publiques que les personnes morales de droit privé chargées de missions de service public.

Les expressions de " traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à sa demande " ou " au respect d'une obligation légale du responsable du traitement " peuvent être reprises littéralement dans la loi. Ces termes clairs permettent par exemple de fonder, dans le premier cas, la collecte de données dans le cadre des formulaires bancaires que doit remplir la personne qui demande l'ouverture d'un compte et, dans le second, les traitements imposés par les obligations déclaratives qui pèsent sur les employeurs en matière fiscale et sociale.

La condition de licéité énoncée au point f) laisse une certaine marge aux Etats membres pour définir les circonstances dans lesquelles – en dehors des cas visés par les points a) à e) – la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées peut justifier, pour autant que les droits des personnes concernées ne prévalent pas, la mise en œuvre d'un traitement.

Le législateur national est appelé à établir, pour transposer cette disposition, une balance entre les intérêts des responsables et les droits des personnes concernées. La directive ne donne à cet égard aucun critère. Le considérant 30 se borne à citer des exemples de cas dans lesquels le point f) pourra fonder la licéité des traitements – les activités de gestion courante des entreprises et autres organismes, la prospection commerciale, la prospection faite par une association à but caritatif ou par d'autres associations ou fondations, par exemple à caractère politique –, en précisant que les traitements en cause devront être mis en œuvre dans le respect de dispositions visant à permettre aux personnes concernées de s'opposer sans devoir indiquer leurs motifs et sans frais au traitement de données les concernant.

Cette clause de sauvegarde, si elle paraît destinée à résoudre des cas résiduels, pourrait, à terme, recouvrir la majorité des traitements du secteur privé. Il est donc nécessaire de l'intégrer à la loi pour fournir un cadre juridique à ces traitements dans le régime issu de la directive.

Il paraît difficile de préciser les termes de la directive sur le nature des " intérêts légitimes " susceptibles de fonder la licéité de ces traitements. L'énumération donnée par le considérant 30 est en effet loin d'épuiser toutes les finalités possibles des traitements mis en œuvre par des opérateurs privés en dehors du cadre d'une relation contractuelle entre le responsable et la personne concernée, ou d'une obligation légale du responsable. Elle omet par exemple de viser les fichiers-témoins, ou *cookies*, mis en place par les serveurs sur le réseau internet pour conserver la trace des sites visités par leurs clients.

La transposition du point f) ne saurait donc conduire à une énumération limitative des finalités

légitimes des traitements qu'il recouvre.

Les motifs de la directive invitent cependant les législateurs nationaux à prévoir des garanties renforcées pour les personnes concernées lors de la mise en œuvre de traitements qui n'entrent dans aucun des cas visés par les points a) à e). Il est proposé d'insérer dans la loi des dispositions aux termes desquelles un tel traitement ne peut être effectué :

–que s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par les tiers auxquels les données sont communiquées,

–à la triple condition qu'il ne porte pas à la vie privée des personnes concernées une atteinte excessive au regard des finalités poursuivies, que ces personnes soient informées du traitement de données les concernant, et qu'elles soient mises en mesure de s'y opposer sans devoir indiquer leurs motifs et sans frais (au moins dans le cas des traitements de données à des fins de prospection ; cf. art. 14, b)).

L'article 14, b) et le considérant 30 ne prévoient une définition aussi large du droit d'opposition que dans le cas du traitement de données à des fins de prospection. Mais l'extension de ce droit à l'ensemble des cas visés par l'article 7, f) – incluant notamment les fichiers-témoins créés sur internet – serait sans doute admis par la Commission.

Il y a donc lieu d'exclure que les traitements de cette catégorie puissent, en application des articles 11, paragraphe 2, et 13 de la directive, bénéficier de dérogations à l'obligation d'informer les personnes concernées prévue par les articles 10 et 11, paragraphe 1, ou au droit d'opposition garanti par l'article 14.

Article 8 : TRAITEMENTS PORTANT

SUR DES CATEGORIES PARTICULIERES DE DONNES

Liste des données sensibles

L'article 8 de la directive énumère six catégories de données dont le traitement est en principe interdit, car elles sont " susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée " (considérant 33).

Cette liste, reprise de la Convention n 108 du Conseil de l'Europe, comprend les données à caractère personnel " qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ", ainsi que les données relatives à la santé et à la vie sexuelle.

La loi du 6 janvier 1978 comporte, en son article 31, une disposition analogue, qui ne visait toutefois, dans sa rédaction initiale, que les quatre premières catégories de données. La référence aux " mœurs " a été ajoutée par la loi du 16 décembre 1992.

Il convient, pour mettre la loi en conformité avec la directive, d'y ajouter les données relatives à la santé. On relèvera cependant que cette dernière catégorie de données se différencie assez sensiblement des cinq autres – dont le traitement menace de manière évidente, et par nature, sauf dans des exceptions très étroitement encadrée, les libertés fondamentales.

En effet, contrairement aux données précitées, les informations relatives à la santé ont vocation à faire l'objet d'un traitement systématique, pour les fins de la médecine, de l'administration du système de santé et d'assurance-maladie, et de la santé publique. Il reste que, détourné de ces finalités, le traitement des données de santé présente des risques considérables pour les libertés publiques. L'apport fondamental de la directive est d'encadrer le traitement de ces données dans

les strictes limites des finalités qui viennent d'être énoncées, et de restreindre les catégories de destinataires habilités à y accéder, par le jeu des exceptions prévues par les paragraphes 3 et 4 de l'article 8.

La directive omet en revanche de se référer de façon explicite à une catégorie de données qui, pour reprendre les termes du considérant 33, sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée. Les risques liés au traitement des données génétiques ont été évoqués en introduction du présent rapport.

La déclaration universelle sur le génome humain, adoptée par la conférence générale de l'UNESCO en 1997, a caractérisé les droits fondamentaux qui devaient être protégés en cas de traitement de données relatives aux caractéristiques génétiques des personnes :

–le génome humain en son état naturel ne peut donner lieu à des gains pécuniaires (art. 4) ;

–une recherche, un traitement ou un diagnostic portant sur le génome humain, ne peut être effectué qu'après une évaluation rigoureuse et préalable des risques et avantages potentiels qui leur sont liés à des fins de conformité avec toutes autres prescriptions prévues par la législation nationale. Dans tous les cas, le consentement préalable, libre et éclairé de l'intéressé sera recueilli (art 5) ;

–nul ne doit faire l'objet de discriminations fondées sur ses caractéristiques génétiques, qui auraient pour objet ou pour effet de porter atteinte à ses droits et à ses libertés fondamentales ou de porter atteinte à sa dignité (art. 6) ;

–la confidentialité des données génétiques associées à une personne identifiable, conservées ou traitées à des fins de recherche ou dans tout autre but, doit être protégée dans les conditions prévues par la loi (art. 7) ;

–pour protéger les droits de l'homme et les libertés fondamentales, des limitations aux principes du consentement et de la confidentialité ne peuvent être apportées que par la loi, pour des raisons impérieuses et dans les limites du droit international public et du droit international des droits de l'homme.

Cette déclaration de droits se fonde sur la nature particulière du génome humain, qui " sous- tend l'unité fondamentale de tous les membres de la famille humaine, ainsi que la reconnaissance de leur dignité et de leur diversité ", et qui, " dans un sens symbolique, est le patrimoine de l'humanité " (art. 1er).

La richesse potentiellement illimitée des informations contenues dans le génome humain, et les relations qu'elles entretiennent avec les caractéristiques les plus intimes de l'identité de l'individu et de son lignage, justifient que ces données jouissent d'une protection exceptionnelle, au même titre que les catégories de " données sensibles " qui viennent d'être évoquées.

Si la directive ne vise pas expressément les données génétiques, plusieurs éléments semblent permettre de les inclure dans le champ de l'interdiction énoncée par le paragraphe 1 de l'article 8 :

–le rattachement du génome humain aux données relatives à la santé constitue, en première analyse, le moyen le plus simple de résoudre la difficulté. Toutefois, la diversité des informations contenues dans un échantillon génétique ne semble pas pouvoir se réduire à une telle définition ;

–le considérant 33, qui vise, de façon globale et sans les énumérer, les données " susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ", offre un fondement possible à la disposition proposée ;

–le paragraphe 7 de l'article 8, qui laisse aux Etats membres toute latitude pour déterminer " les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ", pourrait également fournir une base juridique. En effet, les données génétiques, lorsqu'elles concernent une personne identifiable, pourraient être regardées comme des identifiants de portée générale.

Il est donc proposé d'inclure ces données dans l'énumération des données sensibles dont le traitement est en principe interdit.

Dérogations

Après avoir posé le principe de l'interdiction du traitement des données sensibles, l'article 8 énonce, dans ses paragraphes 2 à 5, huit catégories de dérogations, dont certaines doivent obligatoirement être transposées, alors que d'autres sont optionnelles.

Consentement explicite de la personne concernée

Le paragraphe 2 mentionne en premier lieu, au point a), le cas dans lequel la personne concernée a donnée son consentement explicite au traitement des données. Cette dérogation est conforme à celle que prévoit le premier alinéa de l'article 31 de la loi du 6 janvier 1978, qui se réfère au " consentement exprès de l'intéressé ".

La loi n'a donc pas à être modifiée sur ce point.

La directive ouvre cependant aux lois nationales la faculté de disposer que, dans certains cas, l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée. Cette possibilité pourrait être utilisée à l'égard du traitement de données génétiques, lorsqu'il ne s'inscrit pas dans le cadre d'un traitement médical, de finalités de recherche dans le domaine de la santé, ni d'une procédure judiciaire. En effet, l'importance des risques présentés par le traitement de ce type de données justifie que le consentement des personnes concernées ne puisse être regardé comme suffisamment éclairé pour autoriser tout type d'exploitation, notamment à des fins commerciales.

Cette exception se rattacherait aux règles de droit civil qui posent le principe fondamental de l'indisponibilité du corps humain.

Obligations du responsable en matière de droit du travail

Le point b) du paragraphe 2 prévoit une deuxième dérogation à l'interdiction du traitement de données sensibles, lorsque ce traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates.

Ces dispositions visent notamment les cas dans lesquels la législation nationale prévoit le prélèvement à la source – par l'employeur – des cotisations syndicales ou des contributions fiscales aux Eglises.

Leur transposition n'est pas nécessaire en droit français, dans la mesure où le droit du travail n'implique aucun traitement de données sensibles par les employeurs.

Clause humanitaire

Le point c) prévoit une troisième exception – dite " clause humanitaire " – lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner

son consentement.

Ce cas très particulier n'est pas prévu par l'article 31 de la loi du 6 janvier 1978. Il vise les fichiers des organisations humanitaires sur les personnes arrêtées ou disparues, ainsi que situations d'urgence – notamment en matière de santé – dans lesquelles le consentement de la personne concernée ne peut être recueilli, alors que sa survie, ou celle d'une autre personne, est en jeu.

Cette disposition doit être transposée dans la loi, sous réserve, comme pour l'article 7, d) du remplacement des termes d'" intérêts vitaux " par les mots " sauvegarde de la vie ".

Association à finalité politique, philosophique, religieuse ou syndicale

La quatrième dérogation, énoncée par le point d), reprend celle qui figure au deuxième alinéa de l'article 31 de la loi du 6 janvier 1978. Elle vise le cas dans lequel " le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association, ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées ".

Les dispositions de la directive paraissent cependant plus protectrices des droits des personnes concernées que celle de la loi, qui, faisant prévaloir une conception extensive de la liberté d'opinion et de conscience, prévoit que les traitements en cause ne peuvent être soumis à " aucun contrôle ".

Une telle clause d'exclusion ne peut être maintenue dans le texte modifié en application de la directive que si elle est interprétée comme ne concernant que les formalités préalables et n'excluant pas un contrôle a posteriori. En effet, un tel contrôle est seul à même de garantir que les traitements mis en œuvre, notamment à des fins de prospection, par les partis politiques et par les groupements à caractère religieux, ne sortent pas du cadre strict de la dérogation autorisée par la directive.

En outre, l'interdiction de communiquer les données à des tiers sans le consentement des personnes concernées devra être reprise dans la loi.

Données manifestement rendues publiques par les personnes concernées

Le point e) prévoit deux dérogations de nature très différente.

La première porte sur les données manifestement rendues publiques par les personnes concernées.

Elle permet de résoudre une difficulté posée par l'article 31 de la loi du 6 janvier 1978, qui ne comporte pas une telle réserve, et interdit donc en théorie de mettre en mémoire ou de conserver des données relatives aux engagements d'hommes politiques ou de dirigeants syndicaux de premier plan.

Il est donc souhaitable d'intégrer cette exception dans la loi – et la directive l'impose en tout état de cause.

Il convient toutefois d'en comprendre précisément la portée. L'étendue de cette dérogation doit être appréciée à la lumière du principe de finalité : elle ne signifie nullement que toute donnée sensible manifestement rendue publique par la personne concernée puisse faire l'objet de

n'importe quel traitement. La circonstance qu'un militant ait rendu publiques ses opinions politiques, syndicales, religieuses ou philosophiques, ou encore ses mœurs, n'autorise en aucun cas le responsable d'un traitement à prendre ces informations en compte à l'appui de mesures qu'elles ne sauraient fonder.

Traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice

Le point e) comporte une seconde dérogation, qui porte sur les données dont le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

Cette exception porte sur une matière dont le rattachement au champ d'application de la directive n'est pas évident, l'article 4 en excluant la justice.

Cependant, elle se rattache à la nécessité, pour les professions juridiques – qui entrent dans le champ de la compétence communautaire –, de traiter les informations contenues dans les dossiers de leurs clients, qui peuvent comporter des données sensibles relatives aux intéressés ou à leurs adversaires. Ainsi, un cabinet d'avocats traitant des affaires de responsabilité médicale, ou d'atteinte aux droits de salariés protégés, est-il amené à effectuer des traitements entrant dans le champ de cette dérogation.

Traitement à des fins médicales, par des personnes soumises au secret professionnel

Le paragraphe 3 de l'article 8 pose l'exception la plus importante à l'interdiction du traitement des données sensibles : " Le paragraphe 1 ne s'applique pas lorsque :

–le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé,

–et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente. ".

La transposition de cette dérogation dans la loi du 6 janvier 1978 permettra de compenser l'effet de l'ajout des données de santé à la liste des données sensibles, tout en encadrant strictement le traitement de ces données, désormais restreint à des finalités et à des destinataires étroitement définis.

La limitation par la directive des personnes autorisées à effectuer le traitement des données constitue une garantie essentielle, qui a été intégrée au projet français de ".réseau santé- social " à travers la mise en place d'une " carte de professionnel de santé " permettant de différencier les niveaux d'habilitation des personnes ayant accès au réseau.

Il y a lieu de reprendre littéralement les termes de ce paragraphe dans la loi.

La question du régime de contrôle applicable aux traitements de données de santé sera examinée plus loin, sous les articles 18 à 20.

Motif d'intérêt public important

Le paragraphe 4 autorise enfin une dernière catégorie de dérogations, en ouvrant une assez large marge d'appréciation aux autorités nationales : " Sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle ".

Les considérants 34 à 36 viennent préciser les catégories de traitements de données sensibles qui sont susceptibles de trouver leur justification dans un tel motif. Il s'agit notamment :

–des traitements intervenant dans des domaines tels que la santé publique et la protection sociale – particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de service dans les régimes d'assurance-maladie ;

–des domaines tels que la recherche scientifique et les statistiques publiques (considérant 35) ;

–du traitement de données à caractère personnel par des autorités publiques pour la réalisations de fins prévues par le droit constitutionnel ou le droit international public, au profit d'associations à caractère religieux officiellement reconnues (considérant 36) ;

–de la collecte par les partis politiques de données relatives aux opinions politiques des personnes, dans le cadre d'activités liées à des élections, lorsque, dans certains Etats membres, le fonctionnement du système démocratique le suppose (considérant 37).

La dérogation ainsi posée à l'interdiction du traitement des données sensibles permet de fonder les traitements automatisés de données ayant pour fin la recherche dans le domaine de la santé, autorisés et encadrés par les dispositions des article 40-1 à 40-10 de la loi du 6 janvier 1978 modifiée par la loi du 1er juillet 1994. En effet, ces traitements ne se rattachent pas directement aux " fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé " visées par le paragraphe 3, mais certainement à un " motif d'intérêt public important ".

La finalité des traitements autorisés par la loi du 1er juillet 1994 ne saurait donc soulever de difficulté. En revanche, les dispositions de l'article 40-5 instaurant un droit d'opposition sans " raisons prépondérantes et légitimes " tenant à la situation particulière de la personne et de l'article 40-9 n'autorisant le transfert de données vers un Etat tiers que si " sa législation apporte une protection équivalente à la loi française " s'écartent des dispositions des articles 14, a) et 25 de la directive (cf. nos observations sous les articles 25 et 26).

Compte tenu des applications susceptibles d'être mises en œuvre dans le cadre du projet de " réseau santé-social ", la loi devra également prévoir des dérogations pour les traitements mis en œuvre à des fins de santé publique et de gestion des régimes d'assurance-maladie. En effet, ce dispositif vise notamment à permettre l'automatisation du traitement des feuilles de soins, et peut trouver diverses applications en matière de santé publique qui ne se rattachent pas strictement aux fins énoncées par le paragraphe 3..

La loi doit prévoir des garanties appropriées pour ces traitements. Ces garanties peuvent résider :

–dans la soumission des personnes ayant accès aux traitements à une obligation de secret professionnel, même si les agents en cause (agents de l'Etat et des caisses d'assurance- maladie) ne sont pas des personnels de santé soumis au secret professionnel,

–dans une restriction de l'information accessible aux agents en cause aux données strictement nécessaires aux traitements qu'ils ont vocation à mettre en œuvre, dont le périmètre pourra être précisé par décret,

–dans la soumission à des mesures de contrôle par la C.N.I.L. identiques à celles qui seront prévues pour les traitements médicaux prévus par le paragraphe 3.

Dans un souci de clarté de la loi, il est proposé d'intégrer les finalités de santé publique et de gestion de l'assurance-maladie aux dispositions qui seront prises pour la transposition du

paragraphe 3, en les ajoutant à la liste des finalités de santé qui y est énumérée.

Le considérant 35 ouvre également une faculté de dérogation à des fins telles que la recherche scientifique et les statistiques publiques. On renverra sur ce point aux propositions de l'étude susmentionnée du Conseil d'Etat sur l'accès aux données publiques, qui propose de modifier en ce sens les dispositions de l'article 31 de la loi du 6 janvier 1978, en prévoyant également une dérogation à des fins de recherche historique.

Outre les exceptions prévues directement par des dispositions législatives, le paragraphe 4 autorise également l'intervention de dérogations sur décision de l'autorité de contrôle, sous les mêmes conditions d'un " motif d'intérêt public important " et de garanties appropriées.

La procédure prévue par le troisième alinéa de l'article 31 est conforme à ces dispositions, sous réserve d'un aménagement mineur. Cet alinéa dispose en effet que " pour des motifs d'intérêt public, il peut aussi être fait exception à l'interdiction sur proposition ou avis conforme de la commission par décret en Conseil d'Etat ". Le décret pris sur proposition ou avis conforme de la commission est assimilable à une procédure de codécision associant l'autorité de contrôle au pouvoir réglementaire. Il convient cependant de remplacer les termes d'" intérêt public " par " intérêt public important ".

L'ensemble des dérogations susceptibles d'être prises en application du paragraphe 4, qui viennent d'être évoquées, devront être notifiées à la Commission, en application du paragraphe 6. Cette procédure semble notamment devoir s'appliquer aux dispositions de la loi du 1er juillet 1994, de même qu'aux autres régimes législatifs spéciaux qui seraient susceptibles d'entrer dans le champ des exceptions pour " motif d'intérêt public important ", ainsi qu'aux dérogations prises par décret en Conseil d'Etat sur proposition ou avis conforme de la CNIL.

Le traitement des données relatives aux infractions et aux condamnations pénales

Le paragraphe 5 de l'article 8 prévoit que " le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de garanties appropriées et spécifiques : Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ".

Ces dispositions n'appellent aucune mesure particulière de transposition.

En effet, l'article 30 de la loi du 6 janvier 1978 pose le même principe, en ouvrant une dérogation provisoire au bénéfice des entreprises d'assurances qui a été levée par la loi du 4 janvier 1980 relative à l'automatisation du casier judiciaire.

La faculté de traiter les données relatives aux infractions, condamnations ou mesures de sûreté est certes ouverte par la loi de 1978, sur avis conforme de la CNIL, à toutes les personnes morales – de droit public ou privé – gérant un service public. Cependant, une mission de service public, même lorsqu'elle est gérée par un organisme de droit privé, est toujours placée " sous le contrôle de l'autorité publique " au sens des dispositions de la directive.

Le traitement des identifiants de portée générale

Le paragraphe 7 laisse aux Etats membres toute latitude pour déterminer les conditions dans lesquelles un numéro national d'identification, ou tout autre identifiant de portée générale, peut faire l'objet d'un traitement.

L'article 18 de la loi du 6 janvier 1978 prévoit, à cet égard, que " l'utilisation du répertoire

national d'identification des personnes physiques en vue d'effectuer des traitements nominatifs est autorisée par décret en Conseil d'Etat pris après avis de la Commission ".

La directive n'impose aucune modification de ces dispositions (qui n'imposent au pouvoir réglementaire qu'une simple consultation de la C.N.I.L., et non un avis conforme).

Il convient toutefois de souligner que si les risques liés à l'utilisation du numéro national d'identification revêtaient une assez forte spécificité en 1978, l'évolution des technologies de l'information permet désormais d'identifier les individus avec le même degré de fiabilité à partir d'une recherche multicritères combinant des données aussi courantes que le nom, la date de naissance et l'adresse.

La protection particulière dont bénéficie le NIR ne se justifie donc plus aujourd'hui avec la même acuité qu'il y a vingt ans.

Mais l'évolution des mentalités ne suit pas nécessairement celle des techniques de l'information. Et le refus, encore largement partagé par les citoyens français, d'être identifiés à un numéro de portée générale dans leur rapports avec l'administration, peut fonder à lui seul le maintien de la procédure d'autorisation par décret en Conseil d'Etat.

Article 9 : LIBERTE D'EXPRESSION

Liberté d'expression et protection des données

Le problème de la conciliation entre la liberté d'expression et la protection des données à caractère personnel est sans doute l'un des plus difficiles à résoudre. Il y a en effet une antinomie fondamentale, mais non irréductible, entre la première, qui se fonde sur des possibilités illimitées de rassemblement et de circulation des informations et la seconde qui exige au contraire, pour les données personnelles, de strictes limitations afin d'assurer le respect de la vie privée. La contradiction est aggravée aujourd'hui par le développement rapide de l'informatique, de la télématique et des communications à travers les pays et les continents, dont le réseau Internet est l'un des exemples les plus spectaculaires.

Dans la mesure où la directive se réfère expressément, dans ses considérants, aux principes de la Convention Européenne des Droits de l'Homme, elle ne pouvait faire abstraction de la liberté d'expression, tout en cherchant à la combiner avec les règles qu'elle pose elle- même en matière de vie privée.

Cette question avait déjà été vue et traitée dans la loi de 1978 dont l'article 33 prévoit " que les dispositions des art. 24, 30 et 31 ne s'appliquent pas aux informations nominatives traitées par les organismes de la presse écrite ou audiovisuelle dans le cadre des lois qui les régissent et dans les cas où leur application aurait pour effet de limiter l'exercice de la liberté d'expression ".

Les articles mentionnés concernent les flux transfrontières, le traitement des infractions, condamnations ou mesures de sûreté, et celui des données dites " sensibles " (origine raciale, opinion politique, philosophique ou religieuse, appartenance syndicale ou mœurs).

Cet article a donné lieu a une délibération de la C.N.I.L. en date du 24

janvier 1995 " portant recommandation relative aux données personnelles traitées ou utilisées par des organismes de la presse écrite ou audiovisuelle à des fins journalistiques et rédactionnelles ". Dans ce texte, qui n'a pas de valeur obligatoire, il est rappelé que " la collecte, l'enregistrement et l'élaboration d'informations sont inhérents à l'exercice de la liberté de la presse ". Il est indiqué ensuite que le recours " même à des fins exclusivement journalistiques et rédactionnelles, à des traitements automatisés d'informations nominatives ne dispense pas les organismes de presse de

respecter celles des dispositions de la loi du 6 janvier 1978 non expressément écartées par le législateur " ; toutefois la C.N.I.L. note que l'accomplissement des formalités préalables à la mise en œuvre des traitements ne doit pas conduire à soumettre l'" activité journalistique et rédactionnelle à une procédure d'autorisation " et que la reconnaissance des droits d'accès et de rectification ne doit pas, en s'appliquant " aux documents élaborés par un journaliste et non encore publiés ou diffusés ", aboutir à priver de sa substance la liberté de la presse écrite et de la communication audiovisuelle telle qu'elle est définie par les lois du 29 juillet 1881 et du 29 juillet 1982. Elle en déduisait que la loi de 1978 posait certains " problèmes de compatibilité " avec ces lois.

Elle recommandait en conséquence que soit assurée la sécurité des informations traitées, que les recours, les rectifications ou les réponses intervenues après la publication ou la diffusion des données soit jointes à celles-ci et enfin que chaque organisme de presse désigne un " correspondant de la C.N.I.L. ".

La loi et la recommandation ont été dans la pratique peu appliquées. La directive nous donne ainsi l'occasion de préciser les règles applicables et de rendre sur ce point également le droit plus efficace.

La directive en effet a traité le problème à son article 9, sous le titre " Traitements de Données à Caractère Personnel et Liberté d'Expression " dans les termes suivants : " les Etats membres prévoient pour les traitements de données à caractère personnel effectuées aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions ou dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ". La philosophie générale de ce texte est la même que celle de la loi française : application de la loi à la presse, mais dérogations dans l'intérêt de la liberté d'expression. En raison de la gravité des enjeux, cette disposition est l'une de celles qui ont donné lieu aux discussions les plus difficiles lors de l'élaboration de la directive et aux divergences les plus notables dans sa transposition par les différents pays. Le " groupe de protection des personnes à l'égard du traitement des données à caractère personnel ", créé par l'article 29, a tenté dans une première recommandation du 25 février 1997 de donner des orientations : principe de proportionnalité dans l'octroi des dérogations, en tenant compte notamment des garanties accordées aux personnes par la législation sur la presse (droit de réponse ou de rectification) ; limitations des dérogations et exemptions au traitement de données à des fins de journalisme ; existence de voies de recours efficaces en cas de violation de leurs droits, aucune dérogation ne pouvant être prévue au chapitre III (recours juridictionnel, responsabilité, sanctions).

Pour préparer la transposition de l'article 9 dans le droit français, la mission a profité de la concertation menée en 1996 par le service juridique et technique de l'information et de la communication et elle a consulté à son tour le Conseil Supérieur de l'Audiovisuel, l'Agence France Presse, et des syndicats de presse et de journalistes. A partir de ces consultations et de ses propres réflexions, elle propose au Gouvernement de répondre dans le sens des observations qui suivent aux deux questions essentielles qui se posent : faut-il prévoir un ou deux régimes de dérogation ? quelles sont les dérogations à envisager ?

Faut-il prévoir un ou deux régimes de dérogation ?

La première question se pose parce que, à la différence de la loi française, la directive s'applique non seulement au " journalisme ", mais aussi à l'" expression artistique ou littéraire ". Certains ont pensé que ces deux formules devaient être distinguées, pour des raisons de statut et d'activités. La " presse " ou le " journalisme ", ont dans des pays comme la France, des régimes juridiques propres : loi de 1881 pour la presse écrite, loi de 1986 pour la communication

audiovisuelle, article L 761-2 du Code du Travail pour la profession de journaliste. On fait observer également que la presse fonctionne dans l'actualité immédiate, qu'elle doit obéir à des impératifs de rapidité et qu'elle exerce une mission d'information du public.

Cette dualité de régimes dérogatoires ne s'impose pas, au contraire, pour des raisons de texte et de fond.

Il faut observer en premier lieu que si l'article 9 distingue bien le journalisme et l'expression littéraire ou artistique, elle n'en tire aucune conséquence. Elle prévoit en effet que les dérogations peuvent être prévues " dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ". Cette formule a été mise en facteur commun et la " liberté d'expression " qu'elle évoque s'applique aussi bien au " journalisme " qu'à l'" expression artistique ou littéraire ". Au- delà de cette exégèse juridique, les frontières entre les deux notions tentent à s'estomper, avec le développement de l'histoire immédiate, du journalisme d'investigation, des réseaux multimédias. Il n'y a guère de différence entre un journaliste qui prépare une série d'articles sur une personnalité politique, sur un parti ou sur un segment de population et celui qui envisage sur le même sujet la rédaction d'un livre que les moyens modernes de reproduction et de diffusion permettent de mettre en quelques jours à la disposition du public. De même on peut rapprocher la publication de photographies dans un magazine et dans un album.

Enfin la directive s'applique à l'activité de " journalisme " et non au statut de " journaliste " et comme l'a indiqué la recommandation du Groupe de protection des données du 20 février 1997, elle concerne toutes les formes de médias, y compris la presse électronique.

Ce sont donc les mêmes règles qui devront s'appliquer aux deux catégories mentionnées dans l'article 9, ce qui aura au surplus l'avantage d'éviter de difficiles problèmes de définition.

Quelles sont les dérogations à envisager ?

En revanche il n'est pas possible d'éluder le problème des dérogations à prévoir dans le cadre de ce régime unique.

Un accord se constate entre les parties prenantes sur la nécessité de distinguer dans une entreprise de presse, d'édition ou de communication les activités qui relèvent du commerce et celles qui se rattachent à la rédaction. Les premières doivent être évidemment soumises à l'application de toutes les dispositions de la directive. Il n'y a aucune raison de faire un sort particulier à des entreprises comme telles au motif que par ailleurs elles auraient la presse ou l'édition pour objet. En tant qu'acteurs commerciaux elles relèvent du droit commun. Cette solution concerne par exemple leurs fichiers de personnel ou de clients et d'une façon générale tous leurs fichiers de gestion, ainsi que les traitements à des fins de prospection. Les dérogations ne peuvent donc concerner que l'activité éditoriale.

Elles se limitent, selon l'article 9, aux dispositions des chapitres II, IV et VI (licéité des traitements, flux transfrontières et autorités de contrôle), à l'exclusion, selon le considérant 37, des mesures de sécurité. Le principe de finalité doit être appliqué avec souplesse de même que les règles concernant la durée de conservation. Un fichier de presse peut avoir des finalités diverses et imprévisibles au départ ; toutefois il est bien entendu qu'il doit se rattacher à une finalité globale, celle de l'information et de la diffusion des idées et qu'il ne saurait en aucun cas avoir pour objet des actions de commerce et de publicité. Il faut faire le départ entre les fichiers qui servent à l'auteur pour préparer ses œuvres et ceux qui tendraient à prospecter une clientèle ou à définir des profils. Dans le deuxième cas, les médias doivent être, là encore, soumis au droit commun.

Il ne paraît pas possible de soumettre la collecte des informations au consentement des personnes intéressées ni de leur donner un droit d'accès et de rectification pendant la rédaction et avant la publication de l'œuvre car cela risquerait de limiter la liberté d'expression, comme l'avait d'ailleurs indiqué la C.N.I.L. dans sa délibération. De même, comme le fait déjà la loi de 1978, l'interdiction de collecte des données " sensibles " ne doit pas s'appliquer non plus à la presse, qui les traite au contraire abondamment. On peut considérer que les textes français relatifs au droit de la presse protègent suffisamment les droits de la personne en affirmant le respect de la vie privée et le droit à l'image, et en prévoyant des procédures spécifiques telles que le droit de réponse. Ces textes sont sans doute améliorables, mais ils peuvent et doivent l'être en dehors de la transposition de la directive.

La question des archives des entreprises de communication et des journalistes est plus complexe. On peut considérer que dès lors qu'ils sont archivés, les fichiers ne sont plus dangereux et que ceux qui les ont constitués n'ont pas à être particulièrement protégés. Ici il nous semble que la liberté d'expression doit céder le pas à la protection de la vie privée et que dès lors qu'ils sont versés aux archives, les informations nominatives qui figurent dans des fichiers et qui ont fait l'objet de traitements automatisés, doivent être soumises aux règles qui résulteront de la transposition de la directive.

Les flux transfrontières présentent également une difficulté. Dans une époque de mondialisation et de rapidité des transmissions d'un pays à l'autre, et à travers le monde, il convient de ne pas handicaper la presse française en la soumettant à des formalités et à des contrôles. Il semble que dans ce domaine nous devions conserver l'exception qui figure déjà dans la loi de 1978 et selon laquelle la réglementation de ces flux ne s'applique pas à la presse, qui demeure naturellement soumise aux lois générales sur sa responsabilité.

Les traitements doivent-ils être soumis à des formalités préalables ?

Une dernière question doit être évoquée : les traitements automatisés des données à caractère personnel doivent ils être, dans ce secteur, soumis à autorisation ou à déclaration ? Les organes de presse et les journalistes y sont hostiles, car ils y voient une gêne et éventuellement une entrave à leur liberté. Ils ont sans doute raison. Il faut éviter ici toute procédure qui rappellerait les autorisations préalables et la censure du régime antérieur à la reconnaissance de la liberté de la presse. En revanche une formule, suggérée par certains, pourrait être ici utilisée. Nous avons vu que la C.N.I.L. elle-même, dans sa délibération de 1995, a recommandé aux organes de presse de désigner un correspondant qui en assurerait le respect. Cette formule pourrait être reprise en transposant celle qui figure dans la directive à son article 18 : la notification peut être exclue notamment : " lorsque le responsable du traitement désigne... un détaché à la protection des données à caractère personnel chargé notamment :

–d'assurer d'une manière indépendante l'application interne des dispositions nationales prises en application de la présente directive,

–de tenir un registre des traitements effectués par le responsable...

et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées. "

Cette solution, que nous proposons par ailleurs d'écarter d'une manière générale pour des raisons de principe et d'opportunité, pourrait convenir dans le secteur de la communication. Ce " détaché " ne serait pas en fait un simple correspondant de la C.N.I.L. mais il exercerait par une délégation implicite certains des pouvoirs de contrôle qui lui incombent et cela permettrait d'éviter de soumettre la presse et l'édition à des obligations de notification, qui d'ailleurs jusqu'à

présent ne semblent guère respectées. Ce " détaché " pourrait avoir un statut analogue à celui du " médiateur " que certains journaux ont déjà instauré.

Par ailleurs, la concertation a révélé un certain intérêt pour les codes de conduite prévus à l'article 28 de la directive. De tels codes, soit élaborés, par les professions elles-mêmes et homologués par la C.N.I.L., soit élaborés par celle-ci en concertation avec les professions, permettrait de préciser les droits et obligations des directeurs, des rédacteurs et des citoyens. Cette formule semble envisagée dans d'autres pays, comme l'Italie.

En résumé, l'article 9 de la directive pourrait donner lieu aux mesures de transposition suivantes :

–application intégrale à toutes les activités administratives et commerciales ;

–larges dérogations pour les activités journalistiques et rédactionnelles avant la publication ou la diffusion des articles ou des livres ;

–soumission des archives de ces entreprises au droit commun ;

–non-application des dispositions sur les flux transfrontières ;

–institution de " détachés " à la protection des données à caractère personnel au sein des entreprises de communication ;

–élaboration de codes de conduite.

Articles 10 et 11 : INFORMATION DE LA PERSONNE CONCERNEE

Article 10 : En cas de collecte de données auprès de la personne concernée

Les dispositions de l'article 10 sont pour une large part contenues dans l'article 27 de la loi de 1978.

Il faut seulement ajouter à la liste des informations à fournir à la personne concernée :

–l'identité du responsable du traitement et le cas échéant de son représentant,

–les finalités du traitement auquel les données sont destinées.

Il n'y a pas lieu de prévoir que des informations supplémentaires devront être fournies ou de dispenser le responsable du traitement de la fourniture de ces informations, car cela aboutirait à abaisser le niveau de protection puisqu'une telle communication est prévue par la loi de 1978.

Art. 11 : Lorsque les données n'ont pas été collectées auprès de la personne concernée

L'article 11 n'a pas d'équivalent dans la loi de 1978.

L'article 27 de la loi de 1978 devra être complété par la reprise des dispositions de l'article 11, sans qu'il soit nécessaire de reprendre les dispositions des a, b et c identiques à celles de l'article 10 et figurant donc déjà dans l'art. 27 à modifier comme indiqué ci-dessus.

L'article 11, 2, qui prévoit une dérogation pour les traitements à finalité statistique, ou de recherche historique ou scientifique, devra être repris.

Article 12 : DROIT D'ACCES

Les dispositions de cet article correspondent aux dispositions des articles 34, 35, 36, 37, 38 et 3 de la loi de 1978 – l'article 12 de la directive renvoyant à l'art. 15, paragraphe 1, qui contient la

règle édictée à l'art. 3 de la loi de 1978.

La loi de 1978 prévoit que le droit d'accès s'applique aux traitements dont la liste est publiée en application de l'article 22, liste qui comprend tous les traitements qui doivent être déclarés à la CNIL.

En revanche, le droit d'accès ouvert par la directive est indépendant de cette formalité. En effet, nombre de traitements ne seront plus déclarés à l'autorité de contrôle.

La transposition doit ainsi entraîner la modification de l'article 34 de la loi de 1978, par suppression de la référence à l'article 22.

L'article 36 devra d'autre part être complété par la mention du verrouillage, notion nouvelle introduite par la directive.

Enfin, l'article 38 devra être complété par la mention de ce que le responsable du traitement est dispensé de la notification aux tiers de toute rectification, effacement ou verrouillage si cela s'avère impossible ou suppose un effort disproportionné.

Article 13 : EXCEPTIONS ET LIMITATIONS

Cet article correspond aux articles 39 et 40 de la loi de 1978.

La transposition n'implique pas de modification de l'article 40, qui prévoit que le droit d'accès à des données médicales s'exerce par l'intermédiaire d'un médecin.

La transposition affecte seulement l'article 39. La liste des catégories de traitements pour lesquels les droits de la personne peuvent être limités est plus importante dans la directive que dans la loi de 1978.

Etendre cette liste risquerait d'abaisser le niveau de protection garanti par la loi. Cependant, les traitements qui ont pour but exclusif de lutter contre la fraude fiscale – ce qui exclut la plupart des traitements fiscaux qui ont pour finalité d'établir et de percevoir l'impôt – pourraient bénéficier de l'article 13 de la directive, d'autant que la pratique de l'administration fiscale en matière de droit d'accès aboutit en fait à priver les personnes d'un droit d'accès direct.

Par ailleurs, il y a lieu de tenir compte des critiques faites au droit d'accès indirect tel qu'il est actuellement prévu par la loi de 1978. En effet, la notification aux requérants, sans autre explication, qu'il a été procédé aux vérifications apparaît insuffisante. L'article 39 de la loi de 1978 devrait disposer que les investigations et les réclamations auxquelles il a été procédé peuvent être notifiées au requérant, et des informations devraient être communiquées lorsque cette communication n'est pas de nature à nuire à la sauvegarde des intérêts mentionnés dans l'article 13.

De manière à améliorer le niveau de protection, l'art. 39 devra préciser qu'il est fait un rapport annuel adressé au Président de la République, au Premier ministre et aux présidents des Assemblées de l'application de cet article et que ce rapport peut ne pas être publié en tout ou partie.

L'art. 13, paragraphe 2 doit être transposé intégralement.

Article 14 : DROIT D'OPPOSITION

L'article 26 de la loi de 1978 contient des dispositions analogues à celles de l'article 14 de la directive. L'article 26 devra être complété par celles des dispositions de l'article 14 qui sont

nouvelles.

Article 15 : DECISIONS INDIVIDUELLES AUTOMATISEES

Les articles 2 et 3 de la loi de 1978 sont équivalents. Il n'y a pas lieu à transposition.

Articles 16 et 17 : CONFIDENTIALITE ET SECURITE

DES TRAITEMENTS

Article. 16 : Confidentialité

Sans transposition.

Article 17 : Sécurité

L'article 17 de la directive correspond à l'art. 29 de la loi de 1978. Cet article 29 devra être complété par la mention des notions relatives notamment aux réseaux, à la proportionnalité des mesures de sécurité, et à la sous-traitance – notions visées aux points 1, 2 et 3 de l'article 17.

Articles 18 à 21 : FORMALITÉS

Traits généraux

Ces articles sont ceux qui vont entraîner les plus grands changements dans le système français car ils concernent les deux principales différences entre notre loi et la directive : la diminution du contrôle a priori au profit du contrôle a posteriori et l'égalité entre les secteurs public et privé.

Notre système, qui est inscrit dans les articles 15 à 17 de la loi de 1978, distingue les traitements publics et privés.

Les traitements " opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public " sont soumis à une procédure originale qui commence par un " avis motivé " de la C.N.I.L. ; si l'avis est favorable, la décision est prise par un " acte réglementaire " ; s'il est défavorable, " il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'Etat ". Cette deuxième disposition n'a jamais joué, de sorte que le pouvoir d'avis de la C.N.I.L. est devenu en fait un pouvoir de refus d'autorisation, bien que le terme d'autorisation ne soit pas employé dans le texte, sauf pour les cas où elle émane du législateur (article 15).

Les traitements effectués pour le compte d'autres personnes ne sont soumis qu'à une déclaration, qui " comporte l'engagement que le traitement satisfait aux exigences de la loi ".

Le récépissé doit être délivré " sans délai " et le demandeur peut mettre en œuvre le traitement, sans être toutefois " exonéré d'aucune de ses responsabilités " (article 16).

Le Conseil d'Etat a condamné au début de 1997 une pratique de la C.N.I.L. qui consistait en cas de doute à procéder à un examen de fond de la déclaration : elle doit se borner à vérifier sa régularité formelle. Ainsi a été accentuée la différence de régime entre les secteurs public et privé.

Elle est au contraire atténuée par l'article 17 de la loi qui s'applique aux " catégories les plus courantes de traitements à caractère public ou privé, qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés " ; ils sont soumis " à des normes simplifiées " établies par la C.N.I.L. et donnent lieu à une déclaration elle-même " simplifiée " de conformité à l'une de ces normes.

Le système est ainsi clair et simple :

–secteur public : autorisation, délivrée ou refusée en pratique par la C.N.I.L. ;

–secteur privé : déclaration auprès de la C.N.I.L. ;

–dans les deux secteurs, déclaration simplifiée pour les traitements courants et non dangereux qui font l'objet de normes simplifiées.

La directive a l'avantage d'assimiler complètement les deux secteurs, à l'exception des traitements de souveraineté, qu'elle ne concerne pas. Mais il en résulte une architecture plus complexe.

La déclaration – devenue " notification ", mais l'on peut considérer que les termes sont synonymes surtout si l'on prend en compte la jurisprudence déjà citée du Conseil d'Etat – constitue désormais la procédure de droit commun ; selon les considérants de la directive, elle est " suffisante " pour assurer le respect des règles qu'elle pose.

Toutefois, des possibilités de déclaration simplifiée ou même de dispense de toute déclaration sont également prévues dans certains cas (articles 18 et 19).

A l'autre extrémité de l'échelle de contrainte, " les traitements susceptibles de présenter des risques particuliers au regard des lois et libertés des personnes concernées " donnent lieu à ce qu'elle appelle des " contrôles préalables ".

De grandes différences peuvent apparaître dans les Etats membres en ce qui concerne ces catégories, comme l'avaient craint le Conseil d'Etat et l'Assemblée Nationale.

Notification (articles 18 et 19)

Obligation (article 18, paragraphes 1, 2, 3, 4 et 5)

Selon le 1 de l'article 18, la notification est en principe obligatoire pour les " traitements partiellement ou entièrement automatisés ". Cette formule peut être transposée telle quelle à l'article 16 de la loi, en maintenant la phrase selon laquelle le demandeur n'" est exonéré d'aucune de ses responsabilités ".

Le 5 du même article dispose que les Etats membres " peuvent prévoir " que les traitements non automatisés ou certains d'entre eux font également l'objet d'une notification. Il ne paraît pas souhaitable d'utiliser cette faculté, pour ne pas augmenter encore le nombre des déclarations et ne pas multiplier des formalités qui risquent d'alourdir les charges des citoyens et des entreprises. La question pourra être revue à l'expiration de la période transitoire de 12 ans autorisée par l'article 32 pour la mise en conformité des fichiers manuels avec la directive.

Deux autres cas de dispense générale sont autorisés par les 3 et 4 de l'article 18 :

–" les traitements ayant pour seul objet la tenue d'une registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public et de toute personne disposant d'un intérêt légitime " ;

–les " traitements visés à l'article 8, paragraphe 2, point d) ", c'est à dire ceux qui portent sur des données sensibles et " qui sont effectués dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale ". Cette dispense de déclaration est subordonnée à la condition que " le traitement se rapporte aux seuls membres de

l'organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées ".

Il paraît opportun de retenir ces deux exceptions, toujours dans l'esprit d'éviter une bureaucratie trop lourde et d'alléger les formalités.

La première relève du bon sens : il est inutile de déclarer un traitement portant sur un registre obligatoire et public.

La seconde tend à régler un conflit de libertés : l'interdiction de collecter et de traiter des données sensibles telles que les opinions politiques, les appartenances syndicales et les croyances religieuses ne doit pas avoir pour effet d'empêcher les partis, les syndicats, les églises, de recenser leurs propres membres, à usage interne. La loi de 1978 comprend d'ailleurs à l'article 31, deuxième alinéa, une disposition analogue dont la directive s'est manifestement inspirée et qui va plus loin encore, puisqu'elle ne se borne pas à une dispense de déclaration, mais prévoit une dispense de tout contrôle. Il paraît opportun de maintenir cette disposition, qui a pour objet de favoriser l'exercice effectif de la liberté d'association dans des domaines particulièrement importants. Elle doit cependant être interprétée comme ne dispensant le responsable que des formalités préalables liées au contrôle a priori. En effet, la situation particulière des associations et organismes en cause ne saurait justifier l'exemption de tout contrôle a posteriori.

Forme (article 18, paragraphe 1)

La loi de 1978 semble imposer une déclaration pour chaque traitement. Les représentants des entreprises ont exprimé le vœu que chacune d'entre elles puisse faire, si elle le souhaite, une déclaration unique pour l'ensemble de ses traitements. La directive fait une ouverture en ce sens en autorisant une telle déclaration pour " un ensemble de traitements ayant une même finalité ou des finalités liées ". Il faudrait retenir en tout cas cette faculté ; la directive n'interdit pas, semble t il, d'aller plus loin, en permettant la formule d'une déclaration unique pour une entreprise ou pour un groupe, à la condition bien entendu qu'elle soit à la fois claire et complète. La loi pourrait préciser en outre que la déclaration elle-même et son récépissé pourrait être transmis, comme l'ont prévu des lois récentes, par " voie télématique " (loi du 20 juillet 1992), par " voie informatique " (loi du 31 décembre 1992) ou encore " par voie électronique " (loi du 11 février 1994). C'est une demande des entreprises qui paraît justifiée et dont la satisfaction serait particulièrement bienvenue dans une législation relative à l'informatique.

Contenu (article 19)

L'énumération des informations qui doivent figurer dans la notification, inscrite dans l'article 19 de la directive, ressemble beaucoup à celle qui figure à l'article 19 de la loi pour la déclaration. Notre liste est plus longue, mais ce n'est pas une difficulté puisque celle de la directive ne détermine qu'un minimum. Nous pouvons par ailleurs conserver l'alinéa final de notre texte, qui prévoit des exception en ce qui concerne " la sûreté de l'Etat, la défense et la sécurité publique ", puisque ces matières sont expressément exclues du champ d'application de la directive par son article 3.

Déclarations simplifiées et dispenses de déclaration (article 18 -2)

Il peut paraître surprenant d'assimiler deux situations complètements différentes. Ce n'est pas du tout la même chose, en effet, pour les intéressés de déposer une déclaration simplifiée ou de ne faire aucune déclaration. Mais c'est la directive elle-même qui a procédé à ce rapprochement, en posant pour ces deux catégories des conditions communes, qui sont elles-mêmes au nombre de deux, alternatives ou cumulatives (et/ou).

La première tient à la nature des traitements : il s'agit de ceux " qui, compte tenu des données à traiter, ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées ". Il appartient aux Etats membres de préciser " les finalités des traitements, les données ou catégories de données traitées, la ou les catégories de personnes concernées, les destinataires ou catégories de destinataires auxquelles les données sont communiquées et la durée de conservation des données ".

La directive ne précise pas quelle autorité doit fixer le champ de cette disposition et apporter ces précisions. Mais sa rédaction rappelle celle de l'article 17 de la loi de 1978 sur les " normes simplifiées " établies par la C.N.I.L., même si elle n'utilise pas cette expression : il s'agit " des catégories les plus courantes de traitements... qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés " ; cette expression peut être conservée parce qu'elle est très proche de celle de la directive, à l'exception peut-être du mot " manifestement " ; elle doit l'être, car elle a servi de fondement à la trentaine de normes simplifiées adoptée par la C.N.I.L., dont la rédaction n'est pas interdite par la directive.

C'est ainsi l'autorité de protection qui serait chargée de définir, sous le contrôle du Conseil d'Etat, le champ des dérogations à l'obligation de déclaration de droit commun. C'est elle également, dans les mêmes conditions, qui aurait à préciser si ces dérogations peuvent conduire à une dispense de déclaration, comme elle l'a déjà fait au moins une fois, sans y être expressément autorisée, sous l'empire de la loi de 1978. En effet, la rédaction des normes simplifiées lui permet d'apprécier si la dérogation doit se limiter à permettre une déclaration simplifiée ou peut aller jusqu'à la dispense totale de déclaration.

La seconde condition de dérogation, qui, nous l'avons vu, ne se cumule pas nécessairement avec la première, est au contraire totalement étrangère à la législation française. Il s'agit de l'institution d'un " détaché " – nommé aussi " délégué " par les considérants – " à la protection des données ", qui seraient désigné par le responsable du traitement. Il aurait pour missions d'assurer " d'une manière indépendante l'application interne des dispositions nationales ", " de tenir un registre des traitements " et de " garantir de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées ".

Cette disposition a été insérée à la demande expresse de l'Allemagne, qui tenait à pouvoir conserver une institution à laquelle elle est habituée et qui lui donne satisfaction. La directive ne précise pas son statut. Ce pourrait être un salarié de l'entreprise ou une personne exerçant une profession libérale, un commissaire aux données analogue au commissaire aux comptes, qui pourrait d'ailleurs cumuler les deux fonctions.

Cette idée n'a pas reçu en France une grande audience. Tout au plus certains l'accepteraient si elle avait un caractère optionnel, mais on peut se demander s'il n'y aurait pas alors rupture d'égalité entre ceux qui l'auraient choisie et ceux qui l'auraient refusée. D'autres pensent que ce serait un bon moyen de sensibiliser les salariés à la protection des données personnelles les concernant, dont ils ne saisissent pas toujours l'importance. Mais ce moyen, existe déjà : l'article 432 -2 -1 du code du travail, issu d'une loi du 31 décembre 1992, dispose que le comité d'entreprise " est informé, préalablement à leur introduction dans l'entreprise, sur les traitements informatisés de gestion du personnel et sur toute modification de ceux-ci ". Il faudrait veiller à l'application de ce texte récent et donner une interprétation large de l'expression " gestion du personnel ".

Si elle se rattache en Allemagne à une certaine culture de cogestion, l'institution de ces délégués se heurterait en France à de sérieuses difficultés. La principale tient à l'indépendance que la directive exige à juste titre du délégué. Qu'il soit membre du personnel ou extérieur à l'entreprise, il serait de toute façon rémunéré par celle-ci. La situation n'est sans doute pas sans précédents –

médecins du travail ou experts comptables. Mais il s'agit là de professions réglementées, protégées par l'existence d'un ordre et par un code de déontologie ; il n'en existe pas dans notre matière. Le délégué se trouverait sans doute dans une situation inconfortable face à un ordre du chef d'entreprise qui serait contraire à la loi ou à une norme simplifiée.

Il faut ajouter que ce délégué serait investi d'une véritable mission de contrôle, qu'il exercerait en lieu et place de la C.N.I.L. puisqu'il serait chargé de veiller à l'application de la loi, de procéder à l'" examen préalable " des traitements qui y sont soumis, et d'assurer la publicité des traitements.

Pour l'ensemble des raisons qui viennent d'être indiquées, il ne semble pas que cette institution intéressante puisse être utilement transplantée en France, à une exception près : dans le cas de la presse, ce pourrait être un moyen de concilier la liberté d'expression et la protection de la vie privée (voir nos observations sous l'article 9).

Une dernière observation doit être faite, qui ne relève certes pas de la rédaction de la loi de transposition mais de son application. Il serait souhaitable qu'un grand nombre de traitements soient dispensés de toute déclaration. Nous savons que le nombre de traitements automatisés de données personnelles, sans même évoquer les fichiers manuels, s'élève dans notre pays à plusieurs millions et s'élèvera bientôt sans doute à plusieurs dizaines de millions en raison de l'informatisation accélérée de la société. Il ne serait pas raisonnable d'imposer à leurs responsables de les déclarer tous ni de submerger l'autorité de contrôle sous une marée de documents inutiles. Certains ont exprimé le vœu d'une déclaration obligatoire de tous les traitements, afin de faire de l'autorité de contrôle un observatoire ; mais il vaut beaucoup mieux, dans l'intérêt même des libertés et des droits de l'homme, qu'elle consacre ses efforts et son temps, plutôt qu'à un dénombrement qui ne sera jamais exhaustif à la surveillance efficace des traitements réellement ou potentiellement dangereux.

Autorisations (article 20)

Principes

Cet article important présente une difficulté particulière d'interprétation, et ne sera sans doute pas transposé de façon homogène.

En ce qui concerne la terminologie, il faut constater que la directive emploie l'expression de " contrôles préalables " dans le titre de l'article, celle d'" examens préalables " dans son texte, et que le considérant 54 énonce qu'" à la suite de cet examen préalable, l'autorité de contrôle peut émettre un avis ou autoriser le traitement ". C'est le seul endroit dans lequel soit évoquée l'idée d'une autorisation. Mais nous pouvons en faire état car les considérants ont une valeur importante pour éclairer les directives européennes en cas d'imprécision ou d'obscurité. En l'espèce, le Conseil d'Etat avait noté que le texte " ne détermine pas les conséquences juridiques d'éventuelles conclusions défavorables de l'examen préalable mené par l'autorité de contrôle " ; ainsi a été signalée une ambiguïté qui n'a pas été levée expressément par le texte de la directive, mais qui peut être résolue grâce à ses motifs.

Champ d'application

Le Conseil d'Etat avait également souhaité que la notion de " traitements présentants des risques particuliers au regard des droits et libertés des personnes " soit " précisée par une énumération des principaux traitements ainsi visés ". Là encore, c'est dans les motifs que l'on trouve à cette question au moins un commencement de réponse, au considérant 53, qui évoque la nature, la portée ou les finalités du traitement. Mais le texte s'en tient là et il renvoie aux Etats membres le soin, " s'ils le souhaitent, de préciser dans leur législation de tels risques ". C'est donc à ce travail difficile que devra se livrer le législateur français, car la question touche de près " aux garanties

fondamentales accordées aux citoyens pour l'exercice des libertés publiques ".

Il faut d'abord rappeler qu'un certain nombre de traitements et de fichiers relèvent par eux mêmes et directement du domaine de la loi, comme il a été signalé dans le chapitre relatif " aux principes et méthodes de transposition ". C'est le cas à notre avis des grands fichiers nationaux de police et de sécurité, des traitements mettant en jeu des secrets particulièrement protégés par la loi et des interconnexions de traitements à finalités totalement différentes, comme la protection sociale et la police, enfin de ceux qui se rattachent aux procédures pénales ou aux principes fondamentaux de la sécurité sociale. Cette énumération n'a pas à figurer dans la loi car ce serait modifier ou compléter l'article 34 de la constitution. Mais il faudra conserver la formule qui figure au début de l'art 15 de la loi de 1978 : " hormis les cas où ils doivent être autorisés par la loi, les traitements... ".

Mais il existe d'autres traitements à soumettre à autorisation. La liste des catégories concernées devrait être inscrite dans la loi de transposition, en tenant compte de ce que le considérant 54 dispose que leur nombre " devrait être *très restreint* " parce que, selon le considérant 52, " le contrôle a posteriori par les autorités compétentes doit être en général considéré comme une *mesure suffisante* ".

La directive elle-même, dans son considérant 53, n'en donne que deux exemples : l'exclusion d'un bénéfice d'un droit, d'une prestation ou d'un contrat et " l'usage particulier d'une technologie nouvelle ".

Le Conseil d'Etat, dans son avis déjà cité, en a évoqué d'autres : " les traitements portant sur les identifiants nationaux, sur des données sensibles ou sur des données recueillies en l'absence de consentement de la personne.

On peut retenir la première catégorie.

La seconde pose des problèmes, car parmi les données " sensibles " figurent, selon la convention 108 du Conseil de l'Europe et selon la directive elle-même, les données de santé. Or les secteurs privé et public seront désormais placés sous le même régime, et il ne saurait être question de soumettre à autorisation les traitements de cent mille médecins de ville, qui seront d'ailleurs obligatoires et standardisés. Nous avons vu au surplus que les traitements de données sensibles gérés par des associations pour leurs membres pourraient être exonérés même de déclaration. Sous ces deux réserves, les traitements de données sensibles devraient figurer parmi ceux qui seraient soumis à autorisation, d'autant plus qu'ils ne peuvent être autorisés actuellement que par un décret en Conseil d'Etat pris sur proposition ou avis conforme de la C.N.I.L. et que la convention 108 du Conseil de l'Europe ne les autorise que sous la condition de " garanties appropriées ".

La C.N.I.L. a également élaboré dans une délibération du 14 mai 1996 une liste de traitements à risques particuliers, qui a été reprise dans son rapport annuel.

Cette liste comprend 11 rubriques :

matières ne relevant pas du droit communautaire : " sécurité publique, défense et sûreté de l'Etat ; droit pénal ; contrôle de l'immigration et de la régularité du séjour et du travail des ressortissant de l'union européenne " ;

mise en œuvre de nouvelles technologies ;

données sensibles ;

dérogations aux principes protecteurs des personnes prévues à l'art 13 de la directive (qualité des

données, droit d'information, droit d'accès, publicité des traitements) ;

recours au numéro national d'identification ou à tout autre identifiant de portée générale ;

interconnexion entre fichiers distincts ;

traitements conduisant à des décisions individuelles automatisées ;

exclusion des personnes d'un droit, d'une prestation ou d'un contrat ;

enquêtes statistiques obligatoires ;

traitements concernant la totalité de la population ou une partie largement majoritaire de la population concernée ;

flux transfrontières.

Cette liste paraît un peu longue au regard des objectifs affichés de la directive et des nécessités de la protection des droits et libertés.

Nous proposons de reprendre les rubriques suivantes :

1, à condition de ne pas en donner une interprétation trop extensive, qui couvrirait tous les traitements effectués par l'armée ou la police, dont certains peuvent être anodins, comme ceux des pêcheurs à la ligne ou des coureurs de cross de l'armée, ou des clients d'une cantine militaire qui ont été soumis à autorisation en vertu du critère organique en vigueur jusqu'à présent ;

3, sous réserve pour les motifs déjà indiqués à propos de l'avis du Conseil d'Etat, des données de santé, et de l'exonération pour les membres des groupements politiques, syndicaux ou religieux ;

5 ;
8 ;
10, sous réserve de le limiter à la population nationale comme c'est le cas des fichiers clients d'EDF, exemple cité par la C.N.I.L.

Les autres rubriques appellent les observations suivantes :

il est pratiquement impossible de définir une technologie nouvelle et de toute façon elle ne le reste pas longtemps ; dans le domaine de l'informatique, les technologies nouvelles abondent et se succèdent rapidement ; il vaut mieux exercer sur leur utilisation un contrôle à posteriori efficace pour en déceler les dangers et y remédier. Une telle énumération des traitements soumis à autorisation ne doit pas être éphémère, et bien que la directive elle- même, nous l'avons vu, évoque dans son considérant 53, " l'usage particulier d'une technologie nouvelle ", nous ne pensons pas utile de retenir un concept aussi peu opératoire ;

il ne semble pas que nous utiliserons beaucoup les possibilités de dérogations de l'art 13, sauf pour les traitements de souveraineté déjà mentionnés à la première rubrique de la proposition de liste de la C.N.I.L. ;

les interconnexions sont multiples notamment à l'intérieur d'une même administration et d'une même entreprise et beaucoup ne sont pas dangereuses. Il faudrait limiter le champ des autorisations aux interconnexions de traitements à finalités différentes gérées par des organismes distincts ;

en principe les décisions individuelles automatisées sont interdites sauf dans le cadre d'un contrat conclu à la demande de la personne concernée ou sur la base d'une loi ;

les enquêtes statistiques obligatoires ne paraissent pas nécessiter une autorisation dans la mesure où elle sont en principe fondées sur l'anonymat et où elles sont soumises à la loi de 1951 sur le secret statistique ;

11, il n'est pas possible de soumettre tous les flux transfrontières à autorisation car ils se multiplient et ils ne présentent pas tous les mêmes risques. Leur statut sera d'ailleurs traité à l'occasion de l'examen des articles 25 et 26.

Compte tenu de ces observations la liste des traitements soumis à autorisation pourrait être la suivante :

traitements de souveraineté qui ne relèvent pas du droit communautaire, s'ils présentent par leur nature et leur objet des risques particuliers pour les droits et libertés ;

traitements de données sensibles, sauf s'ils sont obligatoires ou soumis à des normes particulières, ou s'ils sont exonérés de tout contrôle ;

traitements utilisant un identifiant national ;

interconnexion entre fichiers ayant des finalités différentes et gérés par des organismes distincts.

traitements ayant pour objet ou pour effet d'exclure des personnes d'un droit, d'une prestation ou d'un contrat ;

traitements concernant la totalité ou la quasi totalité de la population nationale.

Cette liste ne nous parait conduire ni à une surcharge excessive pour l'autorité de contrôle ou pour les responsables du traitement, ni – et c'est l'essentiel – à un abaissement de notre niveau de protection, compte tenu du renforcement corrélatif du contrôle a posteriori.

Inscrite dans la loi de transposition, elle pourrait être précisée, en tant que de besoin, par un décret en Conseil d'Etat.

Procédure et compétence

Il reste à déterminer selon quelle procédure et par quelle institution les autorisations seront accordées. Sur ces points, la directive laisse une large marge de manœuvre aux Etats membres.

Pour les autorisations qui relèvent du domaine de la loi, le Parlement est évidemment seul compétent. Mais il pourrait être utile de faire passer dans la loi nouvelle une disposition de l'actuel règlement d'application selon laquelle les projets de loi présentés en la matière sont soumis pour avis à l'autorité de contrôle. Sans doute une telle règle n'a-t-elle pas d'effet contraignant, et ne concerne-t-elle évidemment pas les propositions de lois ou les amendements ; mais elle manifesterait l'importance attachée par le législateur aux avis de l'autorité de contrôle.

Pour les autres traitements, on pourrait songer à maintenir la procédure actuellement définie par l'art 15 de la loi de 1978 : avis de la C.N.I.L., et, en cas d'avis défavorable, décret sur l'avis conforme du C.E. Mais, comme il a été dit dans la première partie du présent rapport (" bilan et problèmes "), cette procédure a mal fonctionné et a abouti à de mauvais résultats : conflits répétés entre la C.N.I.L. et certaines administrations, fonctionnement de certains fichiers importants sans autorisation ; défaut de recours et d'arbitrage juridictionnel, les avis défavorables n'étant pas susceptibles de recours, même lorsqu'ils ont des effets juridiques sur le pouvoir de décision, comme l'a rappelé le Conseil d'Etat à propos de cette procédure.

Il serait donc préférable, dans l'intérêt des personnes concernées, des administrations et de la

C.N.I.L. elle-même, de prévoir des procédures plus efficaces.

Pour les traitements de souveraineté exclus de la directive, ce pourrait être un décret en Conseil d'Etat, pris sur l'avis motivé et publié de la C.N.I.L.. Sans doute, un tel avis ne bloquerait-il plus la procédure ; mais sa publication lui donnerait une certaine autorité ; surtout, on ne se trouverait plus dans la situation conflictuelle de la procédure actuelle, qui aurait pour effet, si elle était appliquée, de contraindre le Gouvernement à saisir le Conseil d'Etat et à se conformer à son avis. Il faut observer que plusieurs des lois spécifiques relatives à la protection des données personnelles ont disposé que leur texte d'application serait pris après un avis simple de la C.N.I.L.. La loi de 1978 elle-même prévoit une telle procédure dans son article 18, pour l'utilisation du répertoire national d'identification des personnes physiques.

Quant aux autres traitements soumis à autorisation, le pouvoir de l'accorder devrait être confié à l'autorité de contrôle elle-même, comme le permet la directive. C'est elle en effet qui est la mieux placée pour se prononcer. En outre, il paraît exclu de recourir au décret en Conseil d'Etat pour des traitements purement privés. Cette solution irait également dans le sens de la décentralisation, car au lieu d'obliger les collectivités territoriales à demander au gouvernement de saisir le Conseil d'Etat. en cas de position défavorable de la C.N.I.L., elle leur permettrait de saisir directement le juge d'un recours pour excès de pouvoir.

Une telle solution n'est pas sans précédent : la loi de bioéthique du 1er juillet 1994 a déjà confié à la C.N.I.L. le pouvoir d'autoriser elle-même les " traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé ".

Publicité des traitements (article 21)

L'article 21, paragraphe 2, de la directive pose une règle équivalente à celle qu'énonce l'article 22 de la loi de 1978. Cependant il convient de relever qu'en fait, la liste des traitements n'est pas accessible dans les conditions déterminées par la loi de 1978.

A l'avenir, cette liste mise à la disposition du public sera beaucoup plus courte que celle qui devrait être théoriquement disponible aujourd'hui, puisque peu de traitements seront soumis à une procédure d'autorisation ou de notification. Il sera donc d'autant plus facile de mettre à la disposition du public la liste des traitements soumis à une formalité auprès de la CNIL.

En ce qui concerne les traitements dispensés de notification, l'article 22 de la loi de 1978 devra être complété, pour transposer l'article 21, paragraphe 3, de la directive. A cet égard, l'art. 21 de la directive laisse les Etats libres de prendre des mesures pour assurer la publicité que la publicité soit faite par le responsable du traitement. La loi devrait prévoir la communication, sous une forme appropriée, à toute personne qui en fait la demande, des informations visées à l'article 19, paragraphe 1, points a) à e).

Lorsqu'une personne sera " détachée " à la protection des données, la publicité des traitements sera assurée par le registre des traitements établi sous son autorité.

Article 22 : RECOURS

L'article 22 prévoit la possibilité d'un recours administratif devant l'autorité de contrôle et la nécessité d'un recours juridictionnel " en cas de violation des droits garantis par les dispositions nationales applicables au traitement en question ". L'un et l'autre existent déjà en France.

La seule question qui pourrait être posée est celle de la répartition du contentieux entre les juridictions administratives et judiciaires. Elle doit elle aussi être réglée selon les principes généraux de notre droit. Si le requérant se plaint de la manière dont le traitement est géré par son

responsable, il doit s'adresser normalement aux tribunaux de l'ordre judiciaire si ce responsable est une personne privée et à ceux de l'ordre administratif s'il est une personne publique ou s'il est investi d'une mission de service public. L'assimilation à laquelle procède la directive doit respecter les règles d'ordre public de la répartition des compétences.

Certes on aurait pu songer à unifier le contentieux au profit des tribunaux judiciaires pour deux raisons : parce qu'il s'agit de libertés individuelle et de vie privée et " dans l'intérêt d'une bonne administration de la justice ", comme l'a admis le Conseil Constitutionnel dans ses décisions de 1987 à propos du Conseil de la Concurrence et de 1996 à propose de l'Autorité de Régulation des Télécommunications et comme le législateur l'a décidé également pour la Commission des Opérations de Bourse. Mais ces matières relèvent du droit des affaires, qui est essentiellement privé, et le juge administratif participe en de nombreuses occasions à la protection des libertés individuelles et publiques.

Il n'y a pas de raison en l'espèce de soustraire des décisions de l'autorité de contrôle, qui est une institution de droit public, à leur juge naturel, le juge administratif. Cette solution doit s'appliquer à toutes ses décisions quelles qu'en soient la nature et l'objet (autorisations, normes simplifiées, sanctions, etc.). C'est d'ailleurs celle qui a été retenue pour d'autres autorités administratives indépendantes telle que le Conseil Supérieur de l'Audiovisuel. Comme dans ces précédents, le recours contre les sanctions devra être explicitement qualifié de " recours de pleine juridiction ", afin que le Conseil d'Etat puisse être saisi des questions de fait comme des questions de droit, ce que ne permettrait pas le recours en cassation qui est la règle pour les pourvois dirigés contre les sanctions prises par un organisme collégial à compétence nationale. Ainsi seront satisfaites les exigences de la Cour européenne des droits de l'homme concernant l'existence d'un double degré de juridiction en matière disciplinaire.

Cette solution classique paraît d'autant plus opportune que l'unification du contentieux au profit des tribunaux judiciaires connaît de toutes façons des limites, dans les cas où il y a été procédé : l'exercice du pouvoir réglementaire par l'autorité administrative indépendante et la mise en jeu de sa responsabilité.

L'article sur les recours ne devrait donc donner lieu, en principe, à une transposition explicite que si le législateur entend déroger, sur un point ou sur un autre, aux règles actuelles de droit commun.

Ce pourrait être le cas, à propos de l'art 23 sur la responsabilité, si l'on envisage un regroupement devant les tribunaux judiciaires de toutes les actions en réparation contre le " responsable en traitement ", comme cela avait été fait par la loi du 31 décembre 1957 sur les accidents de la circulation, afin d'éviter des contrariétés de jurisprudence inutiles et non justifiés par la nature du service en cause.

Article 23 : RESPONSABILITE

L'art 23, au contraire de l'art 22, doit sans doute donner lieu à transposition, car il crée une présomption spéciale de responsabilité à la charge du " responsable du traitement " qui n'est pas incompatible avec notre droit, mais qui n'y figure pas actuellement.

En effet, le " responsable du traitement " doit réparation du préjudice subi du fait d'un " traitement illicite " ou de " toute action incompatible avec les dispositions nationales prises en application de la directive ", mais il " peut-être exonéré partiellement ou totalement s'il prouve que le fait qui a provoqué les dommages ne lui est pas imputable ", c'est-à-dire qu'il est dû à la force majeure, au cas fortuit, au fait d'un tiers ou à la faute de la victime.

Comme il a déjà été remarqué par certains commentateurs, cette disposition prête à

interprétation. On peut y voir une application pure et simple du principe de responsabilité pour faute énoncé aux articles 1382 et 1383 du code civil, en raison des références aux traitements illicites et à toute action illégale. Mais dès lors que celui qui doit réparer le dommage est expressément désigné, il s'agit en réalité d'un cas nouveau et particulier de présomption de responsabilité qui devrait être inscrit dans la loi de transposition et éventuellement inséré à l'art 1384 du Code Civil. Pour les motifs indiqués à propos de l'article 22, les actions en réparation contre le responsable du traitement pourraient relever de la compétence des tribunaux judiciaires, quelque soit sa nature, publique ou privé.

Article 24 : SANCTIONS

Sanctions pénales

Le régime répressif français en matière de fichiers informatiques – dont la cohérence avec d'autres dispositions du code pénal comparables est sujette à caution – se caractérise par une grande sévérité, dont le contraste avec une jurisprudence pusillanime est frappant.

Les statistiques du casier judiciaire national montrent, en effet, que de 1991 à 1995, seulement 35 poursuites ont abouti à des condamnations, dont une seule peine d'emprisonnement sans sursis d'une durée de six mois.

Il n'existe en effet guère de politique pénale dans ce domaine où, au surplus, les moyens d'investigation humains et matériels de la police judiciaire sont insuffisants et sous-dimensionnés, eu égard à l'ampleur de l'activité économique liée à l'informatique

Compte tenu de la faible effectivité de la loi pénale en cette matière, il paraît souhaitable d'explorer les voies permettant de mieux sanctionner ces atteintes aux libertés.

S'il paraît nécessaire de ne pas abandonner la voie judiciaire au seul profit d'une régulation administrative, il pourrait cependant être opportun d'assouplir la répression, en distinguant selon que le comportement en cause est manifestement destiné à porter atteinte à la liberté ou qu'il révèle seulement une violation d'une règle de forme (sauf à ce que celle-ci ait entraîné un préjudice, le premier étant toujours puni d'une peine correctionnelle – dont le quantum d'emprisonnement ne saurait dépasser trois ans – le second, d'une peine contraventionnelle.

Il ne s'agirait pas d'un abaissement du niveau de protection, dans la mesure où ces modifications seraient de nature à rendre la loi plus efficace.

La première catégorie de comportements pourrait comprendre les cinq infractions suivantes, actuellement contenues dans le code pénal : la mise en œuvre d'un traitement sans formalité préalable (article 226-16), la collecte frauduleuse d'informations (art. 226- 18), la mémorisation de données sensibles sans autorisation des personnes (art. 226-19), le détournement de la finalité du traitement (art. 226-21) et la divulgation à des tiers non autorisés (art. 226-22).

La seconde catégorie, dans laquelle figureraient l'utilisation illicite du répertoire national d'identification (article 42 de la loi du 6 janvier 1978), le non-respect de l'obligation générale de sécurité (art. 226-17 du code pénal), la conservation de données au-delà de la durée initialement prévue ou accordée (art. 226-20) et l'entrave à l'action de la commission (art. 43 de la loi du 6 janvier 1978), pourrait ne plus être sanctionnée que par les peines prévues pour les contraventions.

Cette solution présenterait l'avantage de permettre des poursuites simples et rapides, le cas échéant par voie d'ordonnance pénale, avec les possibilités de traitement de masse qu'ouvre le jugement des contraventions.

Une telle option pourrait s'accompagner de deux modalités nouvelles de procédure.

Il pourrait d'une part être envisagé de donner à la commission des pouvoirs propres de constation des infractions, notamment en cas d'entrave à l'action de ses agents dans les entreprises. D'autre part, la peine complémentaire d'affichage pourrait être prévue pour les peines contraventionnelles, de même que les peines de publication et de diffusion audiovisuelle actuellement prévues pourraient être étendues.

Parmi les infractions de la seconde catégorie, la distinction entre délits et contraventions pourrait aussi ne s'appliquer qu'au regard du préjudice subi. Ainsi, les infractions n'ayant entraîné aucun préjudice pour les personnes (par exemple, l'omission de modalités de traitement propres à éviter la déformation des informations enregistrées, alors que ces informations ne pourraient en toute hypothèse prêter à confusion) seraient punies des peines prévues pour les contraventions de la cinquième classe, alors que les faits ayant entraîné un préjudice (dans le même exemple, les informations enregistrées, par leur insuffisance, ont entraîné des conséquences patrimoniales graves pour un homonyme complètement étranger au traitement – cf. crim. 19 déc. 1995) relèveraient de poursuites correctionnelles.

Ces aménagements devraient avoir pour corollaire une action de formation spécialisée des magistrats chargés des poursuites et des officiers de police judiciaire saisis de plaintes des particuliers.

Sanctions administratives

Le Conseil Constitutionnel, notamment par ses décisions 88-248 DC du 17 janvier 1989 sur le Conseil supérieur de l'audiovisuel, 89-260 DC du 28 juillet 1989 sur la Commission des opérations de bourse, 96-378 DC du 23 juillet 1996 sur l'Autorité de régulation des télécommunications, a admis la dévolution d'un pouvoir de sanction à une autorité administrative indépendante, en entourant ce pouvoir d'un ensemble de garanties de fond et de forme, transposées de la procédure pénale.

Selon le Conseil Constitutionnel, en effet, la loi peut, sans qu'il soit porté atteinte au principe de la séparation des pouvoirs, doter une autorité administrative indépendante d'un pouvoir de sanction, dans la limite nécessaire à l'accomplissement de sa mission.

Dans la décision du 28 juillet 1989 précitée, le Conseil Constitutionnel considère que " le principe de la séparation des pouvoirs, non plus qu'aucun principe ou règle de valeur constitutionnelle, ne fait obstacle à ce qu'une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dès lors, d'une part, que la sanction susceptible d'être infligée est exclusive de toute privation de liberté, et d'autre part, que l'exercice du pouvoir de sanction est assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis ".

L'exercice de ce pouvoir de sanction se trouve encadré par des garanties analogues à celles de la procédure pénale : principe de non-rétroactivité, principe de nécessité ou de proportionnalité des peines, tirés de l'article 8 de la Déclaration des droits de l'homme et du citoyen, principe du respect des droits de la défense.

S'agissant du principe de légalité des délits et des peines, également applicable aux sanctions administratives, le Conseil Constitutionnel a considéré que " l'exigence d'une définition des infractions sanctionnées se trouvait satisfaite, en matière administrative, par la référence aux obligations auxquelles le titulaire d'une autorisation administrative est soumis en vertu des lois et règlements " (décision du 17 janvier 1989 précitée, considérant no 37).

S'agissant du principe de proportionnalité, le Conseil Constitutionnel a admis que ce principe impliquait qu'en tout état de cause, le montant global des sanctions éventuellement prononcé ne dépasse pas le montant le plus élevé de l'une des sanctions encourues (décision du 28 juillet 1989 précitée, considérant no 22).

Dans la décision du 23 juillet 1996 relative à la loi de réglementation des télécommunications, le Conseil Constitutionnel, tout en validant le pouvoir de sanction reconnu à la nouvelle autorité, a paru poser le principe de non-cumul des sanctions administratives de nature pécuniaire et des sanctions pénales (considérant no 15).

Toutefois, dans sa décision du 28 juillet 1989 susmentionnée, au sujet de la COB, le Conseil constitutionnel avait admis ce cumul, sous réserve du repect du principe de proportionnalité des peines. Il a confirmé cette position dans sa décision DC 97-395 du 30 décembre 1997 sur la loi de finances pour 1998 en considérant que " lorsqu'une sanction administrative " – en l'espèce une amende fiscale – " est susceptible de se cumuler avec une sanction pénale, le principe de proportionnalité implique qu'en tout état de cause, le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues ".

La jurisprudence du Conseil Constitutionnel permet de tirer plusieurs enseignements quant aux conditions auxquelles devra répondre le pouvoir de sanction conféré à la nouvelle autorité de protection.

La procédure de sanction implique en effet, après une mise en demeure restée infructueuse, que le contrevenant reçoive notification des griefs, puisse consulter le dossier, présenter ses observations écrites et orales et se faire représenter ou assister par un avocat.

Parmi les sanctions administratives qu'il convient de prévoir dans la loi de 1978, peuvent figurer sans difficulté les sanctions énumérées à l'article 28 sur l'autorité de contrôle, c'est- à-dire l'ordre de verrouillage, d'effacement ou de destruction des données – qui toutefois, en ce qui concerne ces deux dernières mesures, devrait être confirmé par l'autorité judiciaire – ainsi que l'interdiction temporaire ou définitive d'un traitement, et la possibilité d'adresser un avertissement au responsable du traitement.

Les sanctions prononcées doivent être modulées en fonction de la gravité du manquement constaté (principe de proportionnalité) et pourront être de caractère pécuniaire, alors même que ce manquement constituerait une infraction pénale.

La C.O.B. (art. 5-9 de l'ordonnance du 28-9-1967), le Conseil de la Concurrence (art. 13 de l'ordonnance du 2-12-1986) et le Conseil Supérieur de l'Audiovisuel (art. 42-2 de la loi du 30-9-1996), non seulement disposent de ce pouvoir d'infliger des sanctions pécuniaires mais en usent efficacement, sous le contrôle du Juge.

Ce type de sanction apparaît adapté pour lutter avec succès et rapidement contre les manquements les plus courants.

Les sanctions pécuniaires pourraient être limitées à 5 % du chiffre d'affaires de l'entreprise, et, lorsque le contrevenant n'est pas une entreprise, le maximum serait de 10 000 000 F.

La mise en œuvre de ces sanctions devrait, sans doute, dans la composition future de la C.N.I.L., entraîner la mise en place d'une formation disciplinaire plus restreinte que le collège tout entier. Cette formation pourrait être composée de membres élus par la commission pris, en totalité ou en partie, parmi ceux qui appartiennent au Conseil d'État, à la Cour de Cassation et à la Cour des Comptes, et au moins présidée par l'un d'entre eux.

La sanction devra, bien entendu, être motivée, notifiée aux intéressés et pourra faire l'objet d'un recours de pleine juridiction (cf Cour européenne des droits de l'homme, 23 octobre 1995, *Gradinger c/Autriche*), ainsi que d'une demande de sursis à exécution devant le Conseil d'Etat.

Articles 25 et 26 : TRANSFERT DE DONNEES VERS DES PAYS TIERS

La circulation des données à travers le monde est devenue un problème international majeur dont la difficulté s'accroît avec l'augmentation du volume et de la rapidité des flux.

La loi du 6 janvier 1978 y faisait déjà allusion sous une forme encore modeste : selon son article 24, " la transmission entre le territoire et l'étranger, sous quelque forme que ce soit ", d'informations nominatives faisant l'objet de traitement automatisés privés " peut être soumise à autorisation préalable ou réglementée ", sur proposition ou après avis de la C.N.I.L.. Ce texte n'a guère eu de suite sur le plan national, mais il a été relayé par la convention du Conseil de l'Europe en date du 28 janvier 1981, entrée en vigueur en France le 1er octobre 1985, qui a consacré son article 12 aux " transferts à travers les frontières nationales ". Elle affirme qu'une partie à la convention ne peut interdire ou soumettre à autorisation spéciale de tels transferts à destination du territoire d'une autre partie, " aux seules fins de la protection de la vie privée ". Ainsi était créé, entre les signataires de la convention, un espace de libre circulation des données fondé sur le respect de ses règles par les parties contractantes. Mais la faculté est accordée à celles-ci de déroger à ce principe dans deux hypothèses : si la législation nationale prévoit une réglementation spécifique pour certaines catégories de fichiers et de données, en raison de leur nature, sauf si la réglementation de l'autre partie apporte une " protection équivalente " ; ou si le transfert a pour destination finale le territoire d'un Etat non contractant par l'intermédiaire de celui d'une autre partie.

Par ailleurs, la loi de 1978 a été précisée sur ce point, en ce qui concerne les traitements relatifs à la recherche en matière de santé, par son article 40-9 issu de la loi du 1er juillet 1994, selon lequel la transmission hors du territoire français de données faisant l'objet de tels traitement sous une forme non codée n'est autorisée que " si la législation de l'état destinataire apporte une protection équivalente à la loi française ".

La directive traite à son tour de ce problème dans ses art 25 et 26.

Principes (article 25)

Aucune limitation n'est autorisée au transfert de données entre Etats membres, en raison du principe de " libre circulation des données " qu'elle pose dès son article 1er et qui est l'un de ses principaux objectifs. En revanche la directive interdit les transferts vers un " pays tiers ", c'est-à-dire situé en dehors des frontières de l'Union européenne, sauf " s'il assure un niveau de protection adéquat ". Elle précise que ce caractère s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts, compte tenu de la nature des données, de la finalité et de la durée des traitements, des pays d'origine et de destination finale, ainsi que des règles de droit, des règles professionnelles et des mesures de sécurité appliquées dans le pays en cause.

C'est donc une appréciation au cas par cas qui tient compte à la fois de circonstances particulières au traitement et aux données et des conditions générales prévalant dans le pays destinataire. Les Etats membres et la Commission participent à la mise en œuvre de cette politique. En particulier la Commission peut décider qu'un pays assure ou n'assure pas un niveau de protection adéquat. Dans les deux cas, ses constatations lient les Etats membres.

Tels sont les principes énoncés dans l'art 25 qui doivent être transposés dans le droit national.

Dérogations (article 26)

Il en va de même des dérogations prévues par l'art 26 et qui sont au nombre de 6 :

–consentement de l'intéressé ;

–exécution d'un contrat entre celui-ci et le responsable du traitement ou exécution de mesures pré-contractuelles prises à la demande de celui-ci ;

–nécessité pour l'exécution d'un contrat conclu dans son intérêt, entre le responsable du traitement et un tiers ;

–transfert rendu nécessaire ou juridiquement obligatoire pour la sauvegarde d'un " intérêt public important " ou pour " la constatation, l'exercice ou la défense d'un droit en justice " ;

–sauvegarde de l'" intérêt vital " de la personne concernée ;

–transfert intervenu au départ d'un registre public dans la mesure où les conditions légales pour sa consultation sont remplies (art 26.1).

On retrouve ici les notions de consentement et la plupart des principes de légitimité des traitements insérés à l'art 8.

Un transfert ou un ensemble de transferts peuvent également être autorisés lorsque le responsable du traitement offre des " garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux de la personne ", garanties qui peuvent résulter notamment de " clauses contractuelles appropriées " (art 26.2).

La Commission et les autres Etats membres sont informés de ces autorisations ; " en cas d'opposition... dûment justifiée ", la Commission arrête les " mesures appropriées " (art 26.3).

La Commission peut également décider que certaines clauses contractuelles types présente des " garanties suffisantes " (art 26.4).

Procédures

Au niveau européen

Au niveau européen toutes les mesures prises par la Commission en application de ces dispositions le sont selon la procédure prévue à l'art 31, paragraphe 2, c'est-à-dire sur l'avis du comité de l'art 31 composé des représentants des Etats membres et présidé par le représentant de la Commission ; si les mesures envisagées par celle-ci ne sont pas conformes à l'avis du comité, elles sont communiquées au Conseil, qui les approuve implicitement dans un délai de trois mois ou prend dans le même délai une décision différente à la majorité qualifiée.

Il appartiendra à la Commission, si elle l'estime opportun, d'assurer la publicité de ces décisions, afin d'informer les intéressés, mais c'est elle seule et non les autorités nationales qui peut déterminer les conditions et les modalités de cette publication.

Au niveau national

La directive est ici beaucoup moins précise et contraignante. Elle prévoit que les Etats membres se prononcent sur le caractère adéquat de la protection offerte par le pays tiers et accorde les autorisations nécessaires au responsable du traitement qui propose des garanties suffisantes (article 26.2). Quant aux catégories de dérogations définies par l'article 26.1 et fondée sur des critères objectifs, elles ne nécessitent pas l'intervention de la puissance publique. Lorsqu'une telle

intervention est nécessaire, c'est-à-dire dans les deux autres cas, il reste à déterminer quelle autorité doit procéder aux appréciations de l'article 25 et délivrer les autorisations de l'article 26.2.

On peut hésiter entre deux solutions : une autorité gouvernementale ou l'institution de contrôle.

En faveur de la première, on peut faire valoir que les appréciations sur les régimes étrangers et l'établissement de listes " blanches " ou " noires " peuvent affecter les relations internationales de la France ; en outre le " comité " qui contrôle le système est composé des représentants des Etats.

Mais l'autorité de contrôle est techniquement mieux placée pour traiter de questions qu'elle examine quotidiennement au plan interne, et son intervention permettrait de dépolitiser et de dédramatiser les mesures prises. Elle est en outre informée par les déclarations de traitements, en vertu de l'art 19, paragraphe 1, e), des transferts de données envisagés vers des pays tiers.

Pour les autorisations de l'art 26.2, cette solution est évidente car il s'agit essentiellement de vérifier si les garanties offertes par le responsable du traitement sont suffisantes. Pour l'appréciation du caractère adéquat de la protection offerte par un pays tiers, il s'agit de comparer les règles de ces pays avec les règles européennes et nationales dans un domaine que l'autorité de contrôle est particulièrement bien placée pour connaître.

Dans ce cas, comme dans celui des dérogations à caractère objectif de l'art 26.1, la difficulté sera de déterminer selon quelle procédure l'autorité de contrôle pourrait intervenir. Il ne saurait être question de soumettre à autorisation les quantités considérables de transferts qui se font et se feront de plus en plus chaque jour. Ce serait paralyser des échanges importants et handicaper notre pays. La solution pourrait résider, en dehors des autorisations prévues par les art 20 et 26.2, dans la vérification des déclarations qui, conformément à l'art 19, e), comportent des indications sur des flux transfrontières éventuels. Ce serait le seul cas où l'autorité de contrôle pourrait différer la délivrance du récépissé, pendant un délai à déterminer, en cas de doute sur le niveau de protection offert par le pays destinataire ou sur la validité de la dérogation invoquée, et le cas échéant d'opposer un refus motivé au déclarant. Celui-ci pourrait en outre, bien entendu, demander spontanément son avis sur ce point à l'autorité de contrôle.

Ce sera sans doute une lourde tâche pour l'autorité de contrôle, mais c'est là une conséquence de la mondialisation et du développement exponentiel des réseaux internationaux comme Internet.

Cas particulier de la recherche en matière de santé

Le régime spécial institué par l'art 40-9 de la loi de 1978, issu de la loi du 1er juillet 1994, n'est pas entièrement conforme au régime général prévu par la directive, sur deux points :

–il s'applique aux transmissions " hors du territoire français " et non vers les pays tiers ;

–il exige une " protection équivalente " et non une " protection adéquate ".

Sur le premier point, l'adaptation à la directive est facile et nécessaire ; elle s'imposerait de toute façon sur la base des principes généraux du droit européen.

Le second point est plus délicat. L'exigence d'une protection équivalente est sans doute plus forte que celle d'une protection adéquate ; mais elle est de même nature. On doit constater que la France a établi, pour cette catégorie de traitements, un régime exceptionnel, plus sévère que le droit commun en raison de l'extrême " sensibilité " de ces données. Elle a tout naturellement étendu cette spécificité aux transmissions internationales. Une modification du régime actuel sur ce point serait d'autant moins opportune que la loi du 1er juillet 1994 n'a été mise effectivement en application que tout récemment et qu'elle fera sans doute l'objet d'une révision dans un délai

de cinq ans après son entrée en vigueur, en même temps que celle du 29 juillet 1994 relative au corps humain, qui prévoit " un nouvel examen " à son article 21. Dans ces conditions, la différence entre protection équivalente et adéquate ne paraît pas suffisamment importante pour exiger une mesure immédiate de transposition. Au surplus, l'art 26.1 réserve lui-même " le respect des dispositions nationales prévues en application " des autres dispositions de la directive et la loi de 1994, même si elle lui est antérieure, peut entrer dans cette catégorie.

La procédure prévue par l'article 40-2 est également dérogatoire, puisqu'elle comporte un avis d'un comité consultatif spécial et une décision de la cnil. Mais nous avons vu que la directive ne comporte aucune disposition sur ce point.

Article 27 : CODES DE CONDUITE

Les codes de conduite sont sans doute des instruments aussi utiles que les normes simplifiées pour assurer une application efficace et souple de la loi. Mais, dans notre système juridique il ne peuvent jouer qu'un rôle subsidiaire par rapport aux lois et aux règlements. Sous leur forme pure, ils correspondent en fait à la philosophie anglo-saxonne – et plus particulièrement américaine – de l'" autorégulation ", selon laquelle, à la fois l'élaboration des normes et leur application sont confiés à des organismes privés – professions, syndicats, associations. Cette culture n'est pas celle de la France, ni celle de l'Europe telle qu'elle est exprimée dans la directive, qui est fondée au contraire sur un droit élaboré par le législateur et appliqué par l'administration sous le contrôle des tribunaux.

Les dispositions de l'article 27 sur les codes de conduite sont néanmoins intéressantes et peuvent être utiles.

D'une part, le paragraphe 1 prévoit que " les Etats membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres ". Il s'agit donc seulement de " contribuer " dans un cadre sectoriel à l'application des lois et règlements.

D'autre part, selon le paragraphe 2, les Etats membres prévoient que ces codes, élaborés par des associations professionnelles et des groupements de responsables de traitements, peuvent être soumis à l'examen de l'autorité de contrôle, qui s'assure de leur conformité avec les dispositions nationales.

Enfin le paragraphe 3 prévoit des codes communautaires, approuvés par " le groupe de protection des personnes à l'égard des données à caractère personnel " institué à l'art 29.

Rien n'est dit sur la valeur juridique et la force contraignante de ces codes, qu'ils soient nationaux ou communautaires, ni sur les effets de leur examen par l'autorité de contrôle. Ce silence peut être interprété comme autorisant une distinction entre deux catégories de codes de conduite : les codes purement privés, élaborés et appliqués par une profession, et les codes homologués.

Les premiers existent déjà en France. L'exemple le plus connu est celui du marketing direct, qui a été élaboré en concertation avec la C.N.I.L., et qui a d'ailleurs reçu la consécration d'un prix attribué par celle-ci à l'occasion de son vingtième anniversaire. Mais il n'est pas possible d'infliger des sanctions administratives ou pénales à ceux qui commettraient des infractions à de tels codes.

La seconde catégorie au contraire le permettrait. Dès lors que le code serait approuvé, homologué, " labellisé ", par une décision de l'autorité de contrôle, il deviendrait obligatoire et sa violation pourrait être passible de poursuites et de sanctions. Nous connaissons déjà cette formule avec les codes de déontologie des professions libérales, élaborés par leurs représentants

et approuvés par décret ou par arrêté ; mais dans ce cas, l'élaboration du code est obligatoire et des institutions particulières, les ordres, sont chargés d'y pourvoir.

Dans le cas des codes de conduite, il n'y aurait obligation ni de les rédiger, ni de les soumettre à l'autorité de contrôle. Les représentants des professions que nous avons consultés sur cette question n'ont pas présenté d'objections à la formule de l'homologation, dès lors qu'elle est facultative. Certains y sont même favorables, car ils y voient le moyen de prévenir la coexistence et la concurrence de plusieurs codes dans un même secteur.

Cette formule pourrait s'appliquer notamment à des professions comme celle des journalistes, des avocats ou des médecins, ou encore à des secteurs comme ceux de la banque et de l'assurance.

Quant au codes communautaires, ils pourraient également être introduits dans notre droit par une procédure d'homologation.

Article 28 : AUTORITÉ DE CONTRÔLE

Une opportunité pour la France : repenser la C.N.I.L. ?

La directive impose l'institution d'une autorité de contrôle. Sans doute vaudrait-il mieux dire " autorité de protection " puisque la directive comme la convention du Conseil de l'Europe parlent de protection des personnes, et que dans le langage courant c'est à la protection des données qu'il est fait référence. Sans doute également les responsables de traitements, comme les personnes concernées sont-ils plus friands de l'idée de protection que de celle de contrôle, le contrôle n'étant qu'un des moyens d'assurer la protection, qui fait l'unanimité.

La directive, ainsi qu'il a été dit précédemment, ne fixe que quelques règles générales concernant les pouvoirs de l'autorité. La loi française, et par conséquent la C.N.I. L, sont pour l'essentiel conformes à l'article 28 de la directive.

Plusieurs raisons militent pourtant en faveur d'une réflexion d'ensemble sur la C.N.I.L.

Les dispositions de l'art. 28 constituent un minimum. Un vaste champ créatif est offert à la loi nationale qui n'a été utilisé qu'en partie, par anticipation, par la loi de 1978.

Ce champ reste à explorer : la mission de l'autorité est largement différente de celle de la C.N.I.L. version 1978 car d'une part les traitements du secteur privé et du secteur public sont désormais soumis aux mêmes règles, et d'autre part le régime du contrôle – contrôle a priori réduit, contrôle a posteriori systématique – est substantiellement modifié.

Directive mise à part, il n'était pas possible de faire l'économie d'une réflexion sur le rôle de la C.N.I.L., vingt ans après, surtout eu égard à l'évolution de l'informatique.

Les auditions ont souligné que des modifications de la C.N.I.L. étaient généralement souhaitées et attendues. En revanche les suggestions faites sont très diverses, et pas toujours compatibles entre elles.

Le nom de l'autorité

La Commission Nationale de l'Informatique et des Libertés est un nom prestigieux et connu. D'autres autorités administratives indépendantes ont été débaptisées puis autrement rebaptisées sans que leur autorité et leur efficacité en souffrent en définitive. Le titre actuel de l'autorité aurait eu besoin d'être complété, comme le titre de la loi, qui indique qu'elle est relative à l'informatique, aux fichiers et aux libertés. En effet, la C.N.I.L. n'embrasse pas la totalité des problèmes de l'informatique et des libertés, tandis qu'elle a compétence, et la directive le lui

confirme, à l'égard des fichiers non automatisés. Fort probablement, le public a plus à gagner à conserver un nom qui lui est familier, qui évoque une institution qui a œuvré avec succès à la protection des données, qu'à l'échanger pour un nom plus exact, qui devrait se faire connaître. Sans doute sera-t-il plus simple de passer de la C.N.I.L. I à la C.N.I.L. II qui demeurera, souhaitons-le, l'Académie des Libertés ainsi qu'elle a été tout récemment surnommée, sans modifier son nom.

Conserver le nom de la C.N.I.L. marque à coup sûr la continuité de l'institution.

En réalité la mutation de la C.N.I.L. sera et doit être profonde.

Les missions seront profondément nouvelles, puisque l'informatique a changé, et que le secteur public et le secteur privé seront soumis aux mêmes règles. Les modes d'intervention de l'institution seront profondément différents : le contrôle préalable, qui absorbait sans doute 75 % de l'activité de la C.N.I.L., sera remplacé dans une proportion qui reste à déterminer par un contrôle a posteriori. Bref les futurs membres de la CNIL doivent s'imprégner d'un esprit nouveau.

Composition

Composée de 17 membres, la C.N.I.L. constitue un collège dont la taille ne se retrouve ni dans les autres autorités administratives indépendantes, plus ramassées (Commission des Opérations de Bourse et Conseil Supérieur de l'Audiovisuel : 9 membres, Conseil de la Concurrence : 16 membres, le Conseil siégeant le cas échéant en sections de 3 membres ou en commission permanente comprenant le Président et les deux Vice-présidents), ni chez nos voisins européens où dans beaucoup de cas, une seule personne, assistée de services, constitue l'autorité de protection.

Sans doute, s'il était fait table rase de l'existant, compte tenu des nouvelles missions de l'autorité, celle-ci ne comprendrait-elle probablement pas dix sept membres. Mais aujourd'hui, Petit Parlement ou Académie des Libertés, la C.N.I.L. a su fonctionner à 17. Ce chiffre pourrait donc être conservé.

Une C.N.I.L. ressourcée : dix-sept membres

Si le chiffre de 17 était maintenu, les membres devraient être issus pour une partie d'autres milieux que précédemment. Il doit en effet être observé que les représentants des pouvoirs publics, des juridictions et de l'administration, bref du secteur public, y ont une place prépondérante, et la société civile une place trop réduite, qui ne se justifie plus aujourd'hui. Dans le même ordre d'idées, les juristes sont en situation de quasi monopole, et les informaticiens absents.

On pourrait donc envisager que les trois hautes juridictions n'aient plus qu'un représentant, que les trois membres les remplaçant soient désignés l'un par décret en conseil des ministres (quatre au lieu de trois), un autre par le président du Sénat (deux au lieu d'un) et le troisième par le Président de l'Assemblée Nationale (deux au lieu d'un). Les huit membres ainsi désignés ne devraient pas appartenir à l'une des catégories dont sont issues les autres membres, pour éviter la dérive à laquelle on a pu assister. Il conviendrait également de préciser que ces huit membres devraient être désignés en raison de leur autorité, de leur compétence et en outre, pour la moitié d'entre eux, de leur connaissance de l'informatique – exerçant ou ayant exercé leur activité dans ce domaine pendant une durée qui pourrait être précisée (cinq à dix ans).

Onze membres ?

Une autre solution consisterait à réduire à onze le nombre de membres du collège, qui serait composé d'un député, d'un sénateur, d'un membre du Conseil économique et social, d'un conseiller d'État, d'un conseiller à la Cour de cassation, d'un conseiller à la Cour des comptes, de trois membres nommés par décret en conseil des ministres, un par le Président du Sénat et un par le Président de l'Assemblée Nationale – ces personnalités étant choisies, comme ci-dessus, en raison de leur autorité, de leur compétence et de leur connaissance de l'informatique, exerçant ou ayant exercé leur activité dans ce domaine. Dans cette formule, il pourrait être envisagé que les membres aient des suppléants, pour éviter la paralysie de l'institution du fait de l'application nécessaire d'un quorum. Une commission ainsi restreinte gagnerait en efficacité, chacun des membres ayant un secteur de compétence suffisamment vaste.

Neuf ou sept membres ?

Enfin, pourrait être envisagée une solution alliant un organe délibératif et exécutif ramassé et un conseil consultatif plus important. Le collège pourrait être composé de neuf ou sept membres.

Compte tenu des missions de l'autorité, il est souhaitable de conserver les représentants des trois hautes juridictions, un représentant de l'exécutif et de chacune des assemblées dont le Conseil Économique et Social ainsi que des Présidents des Assemblées, soit neuf membres.

On pourrait cependant supprimer les personnes désignées par les Présidents des Assemblées. En effet dans la mesure où les trois Assemblées sont représentées par l'un de leurs membres, il n'est pas indispensable que les Présidents des deux assemblées parlementaires désignent en outre chacun un membre. Le collège ne comprendrait alors que sept membres.

Auprès de ce collège de neuf ou sept membres, pourrait être constitué un conseil consultatif de trente membres issus des grands corps d'inspection (Finances, Administration, Services Judiciaires, IGAS, Police, Gendarmerie), des professions (Université, barreau, médecins, autres professions libérales), des grands secteurs de l'économie (production, distribution, services). L'institution de ce conseil consultatif, cependant, risque d'entraîner un fonctionnement compliqué.

Le collège pourrait plutôt s'adjoindre des consultants spécialisés (médecins, avocats, journalistes, informaticiens, etc.) pour des missions à durée limitée. Les deux formules ne sont d'ailleurs pas incompatibles.

L'exécutif

Quelque soit le nombre et l'origine des membres de la commission, l'exécutif du collège devrait être également modifié dans le sens d'un renforcement.

A l'instar d'autres autorités administratives indépendantes, le Président et les deux Vice-présidents devraient exercer leur activité à plein temps, quitte éventuellement à faire une exception pour les députés et les sénateurs qui seraient conduits à exercer l'une ou l'autre fonction, de manière à éviter de se passer du concours précieux des élus, et à ne pas en faire des membres à compétence réduite.

Président et Vice-présidents sont actuellement élus par le collège. Abandonner cette tradition pourrait apparaître comme une rupture avec le principe démocratique par excellence qu'est l'élection, qui est également une garantie d'indépendance.

Un Président élu avec difficulté risque cependant de voir son autorité entamée. On observera aussi que les Présidents des autres autorités administratives indépendantes sont désignés, comme également le Président du Conseil Constitutionnel, sans que leur autorité soit moindre.

Durée du mandat

Le mandat des membres de la C.N.I.L. est de cinq ans ; le nombre de mandats successifs n'est pas limité. La limitation à deux mandats successifs paraît souhaitable pour permettre le renouvellement de la commission, comme cela a été souvent suggéré. La durée du mandat pourrait être portée de cinq à six ans comme c'est le cas dans nombre d'autorités administratives indépendantes.

En outre, reprenant les dispositions de l'article 90-1 de la loi du 24 juillet 1986, il pourrait être prévu que le nombre des membres de la C.N.I.L. ayant dépassé l'âge de soixante-dix ans ne serait pas supérieur au tiers des membres de la commission en fonction.

Les pouvoirs de l'autorité

Les pouvoirs en matière de formalités préalables et de sanctions ont été examinés. Il s'agit d'examiner ici les autres pouvoirs dont doit être dotée la C.N.I.L.

Les pouvoirs de contrôle a priori de l'autorité de contrôle étant réduits, il convient de renforcer et d'étendre ses pouvoirs de contrôle a posteriori de manière à maintenir globalement le niveau de protection existant, voire de l'améliorer en le rendant plus efficace.

Pouvoir d'investigation

La C.N.I.L. ne dispose que du pouvoir de faire des vérifications sur place (article 21, 2), et de faire effectuer des missions d'investigation et de contrôle par des magistrats (article 11). L'article 28 de la directive invite à développer ses pouvoirs d'investigation.

La loi devrait préciser les pouvoirs d'enquête à conférer aux membres et agents de la C.N.I.L., en s'inspirant par exemple des articles 45, 46 et 47 de l'ordonnance du 1er décembre 1986 relative à la liberté des prix et de la concurrence, de manière à étendre au maximum ces pouvoirs d'enquête et à assurer le respect des droits des personnes auprès desquelles l'enquête est faite, notamment le principe du contradictoire.

Pouvoir d'injonction

Il s'agit de permettre que des mesures conservatoires puissent être ordonnées en cas d'urgence. A cet effet, l'autorité de protection devrait être dotée du pouvoir d'ordonner les mesures nécessaires justifiées par une atteinte portée au respect de la loi et donc de faire injonction de cesser de mettre en œuvre le traitement considéré. Le juge des référés pourrait être saisi par le responsable du traitement à qui pareille injonction serait faite et qui la contesterait.

Pouvoir de procéder à des contrôles et à des saisies

Le refus de coopérer avec la C.N.I.L. est passible du délit d'entrave. Cela n'est cependant pas suffisant pour permettre des contrôles efficaces. Le temps de l'entrave permet de faire disparaître le corps du délit.

La C.N.I.L. devrait être dotée du pouvoir de procéder à des visites sans l'accord des intéressés et aux saisies nécessaires dans les mêmes conditions que le Conseil de la Concurrence (article 48 de l'ordonnance du 1er décembre 1986) et que la Commission des Opérations de Bourse (article 5 ter de l'ordonnance du 28 septembre 1967) dans le respect des règles déterminées par la jurisprudence du Conseil Constitutionnel.

On rappellera seulement que ces mesures doivent toujours faire l'objet d'une autorisation judiciaire au cas par cas.

Droit d'ester en justice

La C.N.I.L. ne dispose pas du droit d'ester en justice. La directive prévoit que l'autorité de contrôle peut disposer de ce droit, ainsi que du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire (ce que peut déjà faire la CNIL en l'état du droit).

La mise en mouvement de l'action publique appartient au ministère public. Il n'apparaît pas opportun de doter la C.N.I.L. de ce pouvoir, la maîtrise générale de l'action publique revenant aux procureurs, sous réserve des constitutions de parties civiles. Au surplus, il convient d'observer que sous le régime actuel, la commission n'a que rarement fait usage de sa faculté de saisir le ministère public.

La C.N.I.L. pourrait recevoir le droit de se constituer partie civile ou, à tout le moins, sans être partie à l'instance, elle devrait être dotée de la faculté de présenter des observations écrites et orales dans la procédure d'appel de ses décisions prononçant des sanctions pécuniaires, ainsi que dans les procédures pénales. Elle devrait également pouvoir former des recours pour excès de pouvoir contre les actes portant atteinte à son statut ou à ses prérogatives.

Enfin une procédure réglant les relations entre les parquets et la C.N.I.L. devrait être mise au point.

Les services

Le développement du contrôle a posteriori, en particulier des vérifications sur place, nécessitera un renforcement des moyens de la C.N.I.L. notamment en personnel.

La nomination du secrétaire général devrait être faite par décret sur proposition du Président de la C.N.I.L.

Les agents devraient être régis par un statut.

Un service d'inspection doit être mis en place, et comprendre des magistrats – en particulier des juges d'instruction et des substituts – des gendarmes, des policiers, des inspecteurs des finances, des inspecteurs des administrations spécialisées – inspecteurs des affaires sanitaires et sociales, du travail, de la répression des fraudes, des impôts, de l'administration – et des informaticiens.

La déconcentration des services de la C.N.I.L. est également souhaitable. Il serait utile de mettre en place des antennes régionales avec le concours de l'administration et des juridictions, pour que l'autorité ne reste pas " purement parisienne ", comme l'avait craint Bernard Tricot dans son rapport préparatoire à la loi de 1978.

Les relations internationales

La France est souvent représentée dans ses relations avec les institutions internationales (Conseil de l'Europe, Union européenne, OCDE), sur le thème de la protection des données à caractère personnel, par le commissaire du gouvernement auprès de la C.N.I.L.. La situation est équivoque, car le commissaire du gouvernement apparaît souvent comme s'il était le représentant et la voix de la C.N.I.L., alors qu'il n'en est rien. D'autre part la C.N.I.L., sans avoir de statut officiel à l'extérieur des frontières, a noué des relations avec ses homologues étrangers, et certains de ses membres ou de ses agents sont entendus en qualité d'experts par des institutions internationales.

L'ambiguïté entretenue concernant le rôle du commissaire du gouvernement doit être levée.

Une place doit être faite à la C.N.I.L. dans les relations internationales, en tenant compte de sa

qualité d'autorité administrative indépendante qui, par principe, ne saurait recevoir d'instruction du gouvernement, ni le représenter, et de la responsabilité du gouvernement dans la conduite de la politique étrangère, la commission ne pouvant évidémment jouer qu'un rôle consultatif.

Le rapport annuel

Le rapport d'activité doit davantage être conçu comme un aiguillon que par le passé, et devrait dénoncer fortement les abus constatés. La loi pourrait expressément prévoir que le rapport d'activité de la C.N.I.L. peut appeler l'attention du Président de la République, du Premier ministre, du Président du Sénat et du Président de l'Assemblée Nationale, sur les difficultés rencontrées, et leur faire part des améliorations qui paraissent de nature à y remédier.

Outre le rapport annuel par lequel la C.N.I.L. fait connaître les conditions dans lesquelles la loi est appliquée, la sensibilisation de l'opinion pourrait être stimulée par un grand colloque annuel et des réunions régulières.

Le représentant du gouvernement auprès de la C.N.I.L.

Un commissaire du gouvernement siège auprès de la commission (article 9 de la loi de 1978). Il assiste aux réunions. Il peut demander une deuxième délibération, mais cette faculté n'a jamais été utilisée. Le commissaire du gouvernement, selon une dernière circulaire de 1993 du Premier ministre, assure la coordination de l'application de la loi de 1978 au sein des différentes administrations ; à cet effet, des correspondants C.N.I.L. sont désignés dans chaque ministère.

Après avoir été exercé par un directeur du ministère de l'Industrie, et un haut fonctionnaire de ce ministère, la fonction a été confiée à un collaborateur des services du Premier ministre : il est donc rattaché au secrétariat général du gouvernement.

Nombre d'administrations et non des moindres traitent directement avec la C.N.I.L.

Dans la mesure où d'une part la coordination prévue n'est pas toujours assurée compte tenu de l'ampleur et de la difficulté de la tâche, et où d'autre part l'activité de la C.N.I.L. va être consacrée en partie au secteur privé, qui ne peut être contraint de s'adresser à la C.N.I.L. par l'intermédiaire du commissaire du gouvernement, la question du maintien de cet organe se pose.

Si le gouvernement souhaite que l'ensemble de ses départements fassent présenter leurs projets en assurant une certaine harmonie, et maintient le Commissaire du Gouvernement, cela suppose une réforme. Il apparaît nécessaire qu'il soit doté de l'autorité nécessaire que lui conférerait le fait d'être issu d'un grand corps de l'Etat, qu'il se situe à un niveau élevé de la hiérarchie et qu'il dispose d'adjoints et de services suffisants pour couvrir tous les secteurs d'activité de la puissance publique et nouer des relations approfondies avec toutes les administrations et le secteur privé.

De manière générale, et en particulier comme cela vient d'être indiqué à propos des relations internationales, il faut qu'il apparaisse clairement que le représentant du gouvernement auprès de la C.N.I.L. ne fait pas partie de la C.N.I.L., qu'il n'en est pas le porte-parole et que le point de vue qu'il expose n'est pas celui de la C.N.I.L. mais du gouvernement. Si cet organe est maintenu ; sa dénomination devra faire apparaître qu'il est le représentant du gouvernement et qu'il est rattaché à un organisme gouvernemental, tel qu'actuellement le secrétariat général du gouvernement.

Articles 29 ET 30 : GROUPE DE PROTECTION DES PERSONNES

A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Ces dispositions instituent et régissent un groupe composé de représentants des autorités de contrôle et de la Commission et chargé d'examiner des questions d'intérêt commun, notamment

sur la l'harmonisation des législations nationales et les codes de conduite communautaires.

Création originale de la directive obtenue de haute lutte par les autorités nationales, ce groupe a le mérite d'être indépendant, mais il n'a que des attributions de caractère consultatif.

Préfiguration d'une Commission Européenne de l'Informatique et des Libertés, ce groupe ne comportera qu'un représentant par autorité nationale de contrôle. Plutôt que de prévoir une présidence tournante, la directive a fixé le mandat du président – élu – à deux années, renouvelable. Le président disposera d'un pouvoir d'initiative important puisqu'il pourra saisir le groupe de toutes questions.

Les dispositions des articles 29 et 30 n'appellent pas de mesures de transposition, à l'exception du pouvoir de la C.N.I.L. de désigner un représentant au groupe.

La loi nationale peut difficilement orienter le choix de la C.N.I.L. à cet égard. Il est à souhaiter que la C.N.I.L. désigne son Président ou un Vice-président pour le suppléer en cas d'impossibilité, pour siéger dans ce groupe.

En effet, c'est en son sein que seront confrontées les expériences de chacun des pays et déterminées les conditions d'une véritable harmonisation de l'application de la directive.

Article 31 : COMITÉ

Cet article, relatif aux institutions européennes, qui crée un comité composé de représentants des Etats membres, présidé par le représentant de la Commission et chargé de prendre des mesures relatives à l'application de la directive, n'appelle pas de dispositions particulières dans la loi de transposition.

Articles 32 et 33 : DISPOSITIONS FINALES

Article 32 : Dispositions transitoires

Les dispositions transitoires de l'article 32 ont un quadruple objet :

fixer le délai de transposition de la directive, soit trois ans à compter de son approbation ;

prévoir que les dispositions nationales soient accompagnées d'une référence à la directive, qui pourrait en ce qui concerne la France, figurer dans le titre de la loi ;

assurer la mise en conformité des traitements existants avec les nouvelles dispositions dans un délai de trois ans après la date d'entrée en vigueur de la loi de transposition. Cette précision devrait figurer dans cette loi ;

autoriser la mise en conformité des traitements de données contenues dans des fichiers manuels avec les art 6, 7 et 8 de la directive dans un délai de douze ans à compter de son adoption, sous la réserve que les personnes concernées puissent exercer leur droit d'accès et obtenir " la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées d'une manière qui est incompatible avec les fins légitimes poursuivies par le responsable du traitement ". Il paraît opportun de prévoir ce délai de douze ans qui permettra d'appliquer les dispositions nouvelles aux fichiers manuels et qui coïncidera peut-être avec celui de leur disparition.

L'art 32 prévoit également que les " données conservées dans le seul but de la recherche historique " ne soient pas rendues conformes aux art 6, 7 et 8. Il est nécessaire d'utiliser cette exception dès lors que les " garanties appropriées " prévues par la directive figurent dans notre

loi d'archives.

Outre les dispositions transitoires prévues par la directive, la loi de transposition devra en contenir d'autres tirées du droit commun, analogues à celles qui figurent par exemple dans les lois successives sur les établissements classés, pour régler le sort des traitements existants ou en cours d'examen. Les premiers doivent être exemptés de nouvelles formalités s'ils ont été régulièrement autorisés ou déclarés, tout en étant soumis aux règles de fond et aux procédures de contrôle a posteriori contenus dans la loi nouvelle. Les formalités prévues par celles-ci s'appliquent immédiatement aux traitements existants irréguliers, qu'elles soient plus lourdes ou plus légères, ainsi qu'aux modifications des traitements réguliers et aux demandes en cours d'instruction. Pour ces dernières, l'autorité de contrôle pourra procéder à une " requalification " des demandes d'autorisation en déclaration ou inversement.

Article 33

Cet article impose aux Etats membres de communiquer à la commission le texte des dispositions qu'ils auront adoptée ; il n'y a pas lieu de procéder à sa transposition.

Conclusion

ENJEUX INTERNATIONAUX

L'expansion des flux transfrontières et le développement d'internet montrent que la protection des données personnelles ne peut plus être abordée uniquement dans un cadre national ni même européen.

La question de la protection de la vie privée sur internet est particulièrement ardue, en raison du nombre des transmissions, de leur volatilité et de la difficulté de les réglementer et de les contrôler. Elle fait l'objet – outre une étude spéciale confiée au Conseil d'Etat sur les problèmes juridiques posés par le réseau – de réflexions au sein de la Commission européenne, du Conseil de l'Europe et de l'OCDE. La première a notamment souhaité, en janvier de cette année, participer à l'élaboration par le Conseil de l'Europe de " lignes directrices sur la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel dans les inforoutes ". Quant à l'OCDE, elle suit la question de près, et a notamment organisé en février une conférence internationale sur " la protection de la vie privée dans une société de réseaux mondialisée ", destinée à amorcer le dialogue intercontinental sur ces problèmes. Il faut également citer le mémorandum dit de " Budapest-Berlin " de novembre 1996 sur la protection des données dans les télécommunications, qui a été examiné en septembre 1997 par des groupes de travail de la Commission.

Les réactions d'inquiétude soulevées notamment en Amérique du Nord par l'adoption de la directive européenne illustrent l'opposition qui existe entre deux types d'approches : l'une fondée sur l'intervention du législateur et sur la mise en place d'autorités publiques contrôlées par les tribunaux, l'autre fondée sur l'autorégulation assortie de sanctions privées. Si certains pays tiers soulignent l'avantage d'être en présence d'une législation commune à tous les pays membres de la Communauté européenne, d'autres s'inquiètent de l'interprétation qui sera donnée de la notion de " niveau de protection adéquat ".

Il ne fait aucun doute que l'adoption de la directive européenne peut être considérée comme une invitation pour les pays tiers à modifier leur législation en la matière.

Trois types de réactions ont été évoqués lors d'un colloque organisé à l'Université de Montréal fin septembre 1997, sous l'égide de la Commission d'accès à l'information du Québec :

–l'adoption d'un système juridique de protection du type de celui qui existe dans les Etats européens ;

–l'élaboration d'une codification internationale permettant à un grand nombre de pays – notamment ceux dans lesquels tout débat démocratique sur la question paraît illusoire – de s'y conformer s'ils souhaitent participer aux échanges ;

–l'autorégulation préconisée par les Etats-Unis. Celle-ci est fondée sur l'idée que le marché et la confiance des consommateurs constituent la meilleure incitation pour que les entreprises adoptent des pratiques loyales en matière de traitement de l'information.

On commence à assister dans certaines régions à une prise de conscience de la nécessité de contrôler le traitement des informations personnelles, notamment en Argentine, mais aucune mesure concrète n'a encore été adoptée au sein de l'ALENA ou entre les pays d'Asie.

Au sein de l'OCDE, le Canada et l'Australie disposent de législations protectrices qui s'appliquent également au secteur privé. Au Canada, le modèle est la loi québecoise, assez proche du modèle européen.

Aux Etats-Unis, en revanche, le *Privacy Act* ne s'applique qu'au secteur public, qui est assez bien encadré ; mais dans le secteur privé, le niveau de protection est très inégal. Le secteur financier a adopté des règles assez strictes (*Fair Credit Reporting Act*), ainsi que le secteur des télécommunications. Mais prédomine une approche sectorielle où l'on aborde séparément la protection des données médicales, la protection de l'enfance, etc.

La plupart des entreprises américaines adhèrent à des codes. Certains ont valeur obligatoire, et leur respect est placé sous le contrôle de la *Federal Trade Commission*.

L'opposition est donc frappante entre l'approche européenne et la position américaine, que l'on trouve notamment exprimée dans le document de la Présidence intitulé *" A Framework for Global Electronic Commerce* " (1997). Selon ce document, qui contient un chapitre sur la vie privée, le premier amendement à la Constitution exige que la liberté de circulation de l'information soit protégée, et qu'un équilibre soit trouvée entre cette liberté et la protection des droits individuels. La directive européenne y est expressément citée comme " conduisant à des politiques disparates, susceptibles d'entraîner une interruption des flux transfrontières ". Les Etats-Unis affirment leur attachement à une politique fondée sur l'autorégulation et la discipline du marché, et leur volonté de continuer les discussions avec leurs partenaires européens afin d'" accroître leur compréhension de l'approche américaine de la protection de la vie privée ", avec pour objectif de garantir que les critères utilisés pour apprécier le caractère adéquat du niveau de protection " sont suffisamment flexibles " pour s'adapter à l'approche américaine.

Trois étapes se sont ainsi succédé :

–la première, pendant les années 70 et le début des années 80, a été celle de la macroinformatique, de la Convention 108 du Conseil de l'Europe, et de l'émergence des législations nationales, dont la loi française de 1978 ;

–la deuxième, ouverte il y a une quinzaine d'années, a été celle de la microinformatique et de la directive européenne de 1995 ;

–la troisième vient de commencer. C'est celle des réseaux mondiaux et d'internet, qui appelle des réflexions communes et des accords internationaux.