L'informatique menace-t-elle nos libertés ?

Poullet, Yves

Published in:
La télématique. Tome 1 : aspects techniques, juridiques et socio-politiques

Publication date:
1985

Document Version
le PDF de l'éditeur

L'informatique menace-t-elle nos libertés?

POULLET Yves
Directeur du Centre de Recherches
Informatique et Droit, Namur

L'article 1 de la loi française du 6 janvier 1978 énonce le principe suivant : "L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques".

Cet article n'est-il qu'un voeu pieux ? En d'autres termes, l'informatique menace-t-elle réellement et de façon irréversible nos libertés ?

Chacun de nous, Mesdames, Mesdemoiselles, Messieurs, se retrouve dans plus de deux cent fichiers automatisés. Nous connaissons ou devinons certaines de ces inscriptions; le guichet automatique bancaire, la réservation de nos places d'avion, le registre national, la liste du personnel de notre entreprise, le chercheur de têtes, l'hôpital où nous sommes admis pour une fracture du bras ... mais nous en ignorons d'autres; plus grave, nous ignorons quelles données ces fichiers, connus ou inconnus, reprennent, comment et en vue de quoi les données sont traitées et surtout à qui elles peuvent être communiquées. Nous voilà dépossédés de notre image ... Celle-ci circule appauvrie, réduite à quelques données sans que nous ayons prise sur elle. Bref, l'ordinateur fait peur.

On connaît la réaction violente de certains contre l'outil informatique. On rappelle à ce propos le sabotage de quelques centres informatiques de la région Midi-Pyrénées. Plus proche de nous, on entend le slogan "Nos libertés individuelles sont en danger", ou plus précisément "Notre vie privée n'existe plus".

Mais l'approche "Vie Privée" est-elle la bonne ? N'y-a-t-il pas en réalité une manière plus positive de concevoir le développement de l'informatique tout en sauvegardant, voire en accroissant nos libertés. Le développement même de l'informatique ne doit-il pas nous rendre conscients d'autres enjeux bien plus importants pour la survie de nos libertés que la simple question de la défense de notre vie privée ?

Certes, il ne s'agit pas d'être naïf et de croire que l'informatisation libre, le laissez-faire ne comporte aucun danger. Certains l'ont cru. Je me souviens de cet ancien président d'une association de consommateurs qui, invité à parler du même thème que celui que j'évoque aujourd'hui estimait que le développement de l'informatique, dans la

mesure où il permettait la transparence absolue de nos sociétés, était un bien en soi, un facteur de moralisation de la société. Il évoquait à ce propos le précédent de nos sociétés moyennageuses ou la réalité de nos villages où chaque membre de la collectivité connaît tout de tous.

L'argument séduit sans convaincre. L'informatisation ne conduit pas naturellement à la transparence. On constate en effet une marchandisation de l'information qui exclut son accessibilité à tous. "L'information", note MADEC, rapporteur pour le précédent gouvernement français, "s'affirme chaque jour davantage comme une ressource autonome, génératrice de richesse et de pouvoir ... le plus souvent, elle est élaborée dans un cercle restreint de confidentialité au sein d'un groupe fermé". Ainsi, les fichés contrôlent de moins en moins bien les circuits qu'empruntent les données prises sur eux. Ainsi, s'accentue le déséquilibre entre ceux qui savent et ceux qui ne savent pas. Ainsi, la protestation des défenseurs de la "Vie Privée" apparaît d'abord comme une protestation contre l'homme "codé" et une société "kafkaienne".

L'approche positive naïve doit être rejetée; il nous apparaît nécessaire d'exclure également l'approche négative dans laquelle se complaisent trop de défenseurs de notre soi-disant vie privée et de projets ou propositions démagogiques. A cet égard, il est significatif que tous les projets belges mettent sur le même pied l'informatique et les écoutes téléphoniques, mêlant ce qui en soi est une pratique licite de recueillir des informations et ce qui en soi ne peut être tenu que comme un moyen illicite de prise d'information.

L'approche négative se caractérise par une réglementation administrative lourde (contrôle a priori de la création des banques de données par un organe administratif; système d'autorisation et de réglementation du contenu). Elle se caractérise également par la reconnaissance d'un "noyau dur" de données pour lesquelles aucun traitement n'est permis et qui constituent a priori une définition minimale de la vie privée, ainsi les données de la vie sexuelle, les données raciales, syndicales, mutualistes, philosophiques, religieuses, voire "culturelles", les données médicales et celles du casier judiciaire.

Cette approche "Vie Privée", à laquelle seul le législateur belge semble tenir - aucun des textes législatifs étrangers ne se focalisent comme lui sur la seule problématique "Vie Privée" -, cette approche nous apparaît à la fois dangereuse et fausse.

Dangereuse, il est remarquable en effet de constater - et nous pensons en particulier à la proposition VANDERPOORTEN

devenue projet - qu'une fois placés devant la réalité des choses, les responsables politiques doivent convenir :

1. que telles données, pourtant qualifiées d'interdites, doivent cependant pouvoir être traitées par telles ou telles banques de données;
2. que l'application de la réglementation doit souffrir certaines exceptions.

Pour ces deux raisons, on voit la pureté de tous nos projets belges se dissoudre dans une multiplication d'exceptions dont l'importance de certaines apparaît comme une remise en cause du principe lui-même. J'en donnerai deux exemples, tirés de l'actuel projet belge.

Premièrement, on affirme que tout traitement doit être soumis à contrôle, mais pour ne pas surcharger les contrôleurs (qu'on songe au développement considérable de la micro-informatique bientôt à la disposition de tous), on exempte de toute réglementation certains traitements a priori peu dangereux, notamment, les traitements de données "ayant fait l'objet d'une publicité légale ou volontaire", ce qui vise certainement les millions de petits agendas automatisés, mais peut recouvrir aussi les listes d'adresses plus sophistiquées d'éditeurs professionnels, étant donné l'imprécision des termes. Ensuite, qu'est-ce qu'une donnée publique ? Les condamnations judiciaires ne sont-elles pas des données publiques ?

Deuxièmement, la défense de la vie privée passe, selon le projet, par la reconnaissance d'un "noyau dur", c'est-à-dire d'une liste de données à propos desquelles aucun traitement n'est en principe possible. Le projet gonfle la liste de ces données mais concurremment, se voit forcé de multiplier les exceptions pour prendre en considération les besoins légitimes de certains organismes. On s'inquiète là aussi. Ainsi les données du passé judiciaire pourront figurer sur les traitements destinés à assurer la sécurité du crédit ... Qu'est-ce qu'un traitement destiné à assurer la sécurité du crédit ? Toutes les données peuvent-elles y figurer ? Pour quelle durée ?

Plus fondamentalement, l'approche "Vie Privée" est fausse. Dans le premier rapport de la C.N.I.L., JOINET, pourtant peu suspect d'être un défenseur des multinationales et autres, faisait remarquer à propos de l'approche "Vie Privée" et de la définition d'un noyau dur de données : "Immanquablement, des interdictions plus larges devraient être accompagnées d'exceptions et pourraient facilement être tournées et surtout, ajoutait-il, *l'adéquation des données à la finalité du traitement* est "une idée directrice plus féconde que les interdictions a priori"".

En fait que craignons-nous lorsque certaines données nominatives telles les données politiques ou syndicales circulent ? Que notre vie privée soit mise en danger ? Il n'est pas rare que certains affirment leur opinions politiques ou syndicales et pour celui qui se présente aux élections y compris les élections sociales, cette donnée est publique selon le voeu de la loi et les exigences de la démocratie. La question n'est donc pas là. Ce que nous craignons, c'est que l'utilisation de la donnée par le ficheur ne puisse être source de discrimination et il y aura, nous semble-t-il, possibilité de discrimination si la présence de telle donnée dans un fichier n'est pas pertinente par rapport au but pour lequel le fichier a été constitué.

Ainsi, que ma banque garde sur moi trace d'une émission de chèques sans provision m'apparaît normal, mais qu'elle la garde indéfiniment remet en cause de façon illégitime ma liberté d'obtenir du crédit. C'est que la conservation d'une telle donnée au-delà d'une certaine durée n'apparaît plus pertinente. Il n'est pas question ici de "Vie Privée", mais de ma liberté économique d'obtenir du crédit. Pour reprendre un exemple relatif à une donnée appartenant au "noyau dur", la donnée syndicale figurant dans les renseignements demandés ou traités lors de mon embauche est non pertinente. Mais pour des raisons légales (paiement d'une prime syndicale) ou en accord avec le syndicat (réglement de certaines cotisations sociales) la même donnée peut figurer dans le fichier de l'entreprise sous certaines conditions, par exemple de non-communication à des tiers et d'accès limité.

Une donnée brute, on le pressent à travers ces exemples, n'est pas une information : il lui manque un sens. Dans ces conditions, préciser la notion d'information revient à mettre en évidence les réseaux de décision dans lesquels les données deviennent utiles. C'est là que porte le débat. Comme le montre l'expérience vécue à l'étranger, les fichiers "sensibles" ne sont pas ceux qu'on croyait. Bien plus par exemple que les fichiers de police, les dangers viennent en pratique des fichiers de sécurité sociale et surtout des fichiers de données banales, même non nominatives. Recoupés avec soin pour un usage abusif, ils peuvent alors constituer un danger majeur. Bref, ce n'est pas la question de la vie privée du fiché qui est en jeu mais bien, de façon plus générale, celle des libertés individuelles et dès lors, comme le notait JOINET, celle des limites au "droit à l'information" des ficheurs. C'est ce "droit à l'information" que le fiché prétend vouloir contrôler lorsqu'il réclame de connaître les informations

contenues dans un fichier à son propos. Le "droit à l'information" du fiché opposé au droit à l'information du ficheur prend alors tout son sens. Ce que le fiché désire, ce n'est pas simplement pouvoir rectifier ou compléter les données éventuellement incorrectes ou incomplètes, mais d'abord contrôler et éventuellement contester, au nom du respect de ses libertés, le droit à l'information de tous ceux qui prétendent utiliser cette information.

Ainsi la question de l'informatique et des libertés individuelles doit se résoudre par la conciliation et la définition de deux droits.

1. Le droit à l'information du ficheur : quel en est le fondement ? Quelles conséquences en tirer ?

2. Le droit à l'information du fiché : quelles en sont la signification et la portée ?

Comment et qui tranchera ce débat, qui définira le droit à l'information des ficheurs et ses limites. Il ne peut être question de le trancher une fois pour toutes en vertu de réglements qui ne pourraient prendre en considération l'évolution de la technique, l'évolution des besoins légitimes des ficheurs et des mentalités. Toute loi relative à la réglementation de l'informatique doit se limiter à l'énoncé de principes que les lois, règlements et décisions jurisprudentielles ultérieurs viendront préciser. Ainsi, note BURKERT, "il est important que la société puisse s'adapter à la technologie de façon à en prendre les avantages et que la technologie puisse s'adapter à des valeurs de base de notre société pour assurer une cohérence sociale dans un environnement changeant". A cet égard, je noterai qu'en Belgique, tous nos projets adaptés au contrôle des gros centres de traitement de l'information facilement localisables, se révèlent peu aptes à réglementer l'existence d'une informatique de poche, peu localisable.

Cette définition et cette conciliation ne sont possibles que par la reconnaissance d'une responsabilité collective qui suppose l'existence d'un organe de contrôle créé, organe reconnu indispensable par tous les textes de lois en vigueur autour de nous.

Si donc nos lois ne peuvent avoir pour ambition de tout réglementer sous peine de devoir échouer en tout, elles doivent mettre en place les outils de la transparence; il faut que les citoyens puissent connaître dans toute la mesure du possible ces circuits d'information qui les environnent et que la question du droit à l'information des ficheurs soit posée publiquement. Ceci exclut que la

solution soit confiée à un organe administratif inaccessible qui enfermera le débat au lieu de le porter sur la place publique. Une telle responsabilité doit être confiée aux organes constitutionnels classiques qui garantiront ce débat public et motivé : le législatif et le judiciaire. Que ceux-ci en même temps que le public doivent être aidés et alertés par une sorte d'ombudsman qui "contribuera à définir progressivement les voies d'une informatique au service d'un citoyen moins fasciné par cette technique et plus responsable", comme se définit la CNIL (second rapport) nous apparaît indispensable.

J'aborderai successivement ces points. Leur examen révèlera que d'autres enjeux sont en cause dans la réglementation de l'informatique et que la question des libertés individuelles n'est pas l'unique problème soulevé mais qu'apparaissent en outre certaines questions de libertés collectives voire publique auxquelles nous devons être particulièrement attentifs dans le futur.

1. LE DROIT A L'INFORMATION DU FICHEUR

On distingue traditionnellement deux types de fichiers : les fichiers publics et les fichiers privés. Cette distinction apparaît fondée, le principe même du droit à l'information pour chacun de ces fichiers n'étant pas le même. Dans le cas de fichiers publics, le droit à l'information indispensable pour assurer un service public efficace s'appuie sur *les principes constitutionnels de proportionnalité, de légalité et de spécialité*; dans le cas de la plupart des fichiers privés, le droit à l'information s'appuie sur *l'existence d'une relation contractuelle* voulue par le fiché et les exigences de sa bonne exécution.

Quelques commentaires à propos de ces principes. Pour les fichiers publics, les trois principes rappelés ci-dessus ont, me semble-t-il, pour conséquence :

- Premièrement, que toute banque de données doit être créée sous le contrôle du législatif.

De façon générale, ce principe exige une certaine coordination et un contrôle de l'informatisation du secteur public. Il importe que le législatif puisse connaître à tout moment les circuits d'information existants ou projetés à l'intérieur des administrations. La question évoquée déborde largement la question des libertés individuelles. Il

s'agit bien plutôt d'une question d'équilibre des pouvoirs et donc de libertés publiques. En effet, l'utilisation croissante de l'informatique dans le secteur public renforce les pouvoirs d'action de l'exécutif central et au sein d'eux, de certaines administrations. Il modifie l'équilibre des pouvoirs, garant traditionnel de la démocratie. Il est donc important que le législatif via l'organe de contrôle puisse contrôler le développement de l'informatisation du secteur public. A cet égard, on peut regretter que l'Arrêté Royal belge du 12 mai 1981 relatif à la coordination et aux moyens de contrôle de l'informatique dans les services publics n'ait pas instauré ce moyen de contrôle, ni cette transparence du parc informatique public, ce que les lois françaises, mais surtout américaines, prévoient explicitement et que le législateur italien envisage par un vaste projet d'informatique parlementaire.

- Secondement, que le fait qu'elle ne puisse enregistrer des données que dans le cadre de la mission qui lui a été confiée (principe de spécialité) et pour autant que cela lui est nécessaire (principe de proportionnalité) exige que la finalité de chaque banque de données publiques soit clairement mise en évidence.

A ce propos, on peut citer à titre d'exemple, la loi créant le "Registre National". A mon sens, la question importante n'était pas de savoir si l'enregistrement de 6 ou 33 données devait être permis, mais plutôt de décider clairement quelle devait être la finalité d'un tel fichier. S'il s'agit, comme le dit l'exposé des motifs, non point de rendre des services aux communes, mais bien de faciliter la tenue à jour des fichiers de l'ensemble des administrations publiques de l'état central, il est nécessaire que les seules données d'utilisation fréquente y soient mentionnées. La prise en considération de cette même finalité exige que le numéro d'identification ne puisse servir que dans les relations entre chaque organisme public de l'état central et le Registre National.

Dans le secteur privé, "le service attendu de l'entreprise collectrice des données est à la fois la justification et la limite de l'usage des renseignements" concluait déjà le rapport TRICOT. Ce principe de pertinence est repris par les lois allemandes, autrichiennes, danoises et norvégiennes.

A la base de la nécessaire consécration de ce principe, repose la constatation suivante : "il ne faut pas perdre de vue que c'est toujours dans un but bien déterminé que

les données sont rassemblées, mises en mémoire et communiquées. *C'est seulement lorsqu'on connaît cet objectif et non en raisonnant dans l'abstrait sur l'information elle-même, que l'on peut tracer la limite de tolérance acceptable pour l'intéressé" (rapport TRICOT).*

Certains objecteront l'imprécision du principe. La notion de "pertinence", disent-ils, est singulièrement floue et son emploi crée le risque d'une interprétation fort large. La critique nous apparaît peu fondée. *Le critère de la "pertinence" est en effet plus souple et plus respectueux d'une appréciation judiciaire évolutive que le critère a priori, réglementaire, tiré de la nature soi-disant "en soi" des données, critères, qui, par opposition, est peu soucieux de la réalité contractuelle.*

Il est évident que ce principe est inapplicable lorsque les données sont enregistrées en dehors de toute relation contractuelle, ainsi que dans le cas d'éditeurs d'adresses, de chercheurs de têtes et d'agences de renseignements commerciaux. Tels fichiers sont soigneusement distingués des autres fichiers privés et objet d'une réglementation a priori dans la plupart des législations étrangères. Il semble que le projet GOL les distingue également en ce qui concerne toute une série d'obligations imposées aux "ficheurs".

Le "droit à l'information" des entreprises et de l'administration entraîne pour elles certaines conséquences relatives à l'utilisation de ces données.

A. Elles sont responsables de la sécurité de leurs fichiers. L'article 7 de la Convention du Conseil de l'Europe mentionne : "des mesures de sécurité *appropriées* sont prises pour la protection des données contre la destruction accidentelle ainsi que contre l'accès, la modification ou la diffusion non autorisés".

Cette question de la sécurité exige :

- la consécration de règles déontologiques applicables à toutes les personnes qui ont à approcher les banques de données;
- pour les centres de traitement localisables, la nomination de "gestionnaires" au sens des projets MOUREAUX et GOL, c'est-à-dire des personnes chargées au sein des entreprises et administrations du respect de la réglementation de l'informatique dont le statut doit être proche de celui des commissaires réviseurs;
- la définition progressive de normes de sécurité nationales et internationales pour les programmes traitant de données nominatives.

B. Le droit à l'information des entreprises ou administrations doit être soigneusement distingué du droit de communication. "La règle posée ci-dessus, à savoir le principe de pertinence, explique le rapport TRICOT, implique que les renseignements possédés par une entreprise et recueillis à l'occasion d'un contrat particulier ne doivent pas être diffusés à des tiers". Cette remarque justifie la différence que toutes les législations y compris le projet GOL font entre le traitement interne d'une donnée et sa communication, en contrôlant plus sévèrement cette dernière. Ainsi, selon la loi allemande, une entreprise n'a droit à la communication de données venant d'une autre entreprise qu'à la condition qu'elle soit conforme dans le chef de la seconde entreprise au but contractuel à la base du traitement des données, mais en outre qu'elle soit justifiée dans le chef de la première par la protection d'intérêts légitimes dans son chef ou dans le chef d'un tiers. Par exemple, selon la jurisprudence allemande, une banque à laquelle un nouveau client venant d'une autre banque demande l'ouverture d'un compte bancaire doit pouvoir obtenir de cette autre banque les données relatives à d'éventuelles émissions de chèques sans provision.

2. LE DROIT A L'INFORMATION DES FICHES

Le droit à l'information des fichés doit se définir de façon large comme le droit de la personne fichée à "participer à la formation de l'image que les personnes qui l'entourent se font de lui". Ainsi présenté, le droit d'information se présente comme le juste corollaire du droit à l'information du collecteur.

Avant d'aborder les différentes facettes de ce droit, il est important de s'interroger sur la notion de fiché. En effet, la réduction du débat "Informatique et libertés" à la seule problématique "Informatique et vie privée" a amené une première génération de lois à exclure de toute protection les personnes morales et les associations et à réserver aux individus, seuls dotés de vie privée, le bénéfice de la loi. A partir du moment où le droit à l'information est consacré en tant que tel, on peut se demander s'il ne peut pas être étendu aux associations et entreprises. Il s'agit de permettre aux entreprises comme aux personnes de protéger leur "goodwill", leur bonne réputation. Ce droit des entreprises à la bonne réputation apparaît comme un corollaire à la fois du principe de l'égalité et de celui de la *liberté d'entreprendre* ou du "droit à l'existence" des entreprises. L'entreprise n'a-

t-elle pas le droit de protéger son existence contre des décisions mal fondées dans la mesure même ou ces dernières peuvent remettre en cause sa survie ?

Ceci dit, deux principes fondent le droit à l'information des fichés.

Le premier principe dit de la "Data Quality" exige que l'information sur laquelle le ficheur basera son éventuelle décision soit, dans toute la mesure du possible, précise, complète, mise à jour et exacte. On remarquera que l'énoncé de ce principe consacre explicitement le droit à l'information des ficheurs puisqu'il le rend responsable de la qualité des données.

Le second principe est le complément du premier, il s'agit du principe énoncé par l'article 2 de la loi française et dont la C.E.E. aimerait étendre l'application à l'ensemble de l'Europe : "Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé". C'est, en d'autres termes, la condamnation du crédit scoring ou du profil de carrière, c'est l'affirmation du droit de chaque personne de contester les "vérités" sorties de l'ordinateur.

Les deux fondements notés, quelles sont les différentes modalités du droit à l'information du fiché ?

- C'est d'abord, lors de la collecte des renseignements, le droit pour le fiché de savoir pourquoi on l'interroge, en quoi la réponse est obligatoire, à quoi et à qui elle servira.

- C'est ensuite, pour le public en général et chacun en particulier, le droit de connaître le degré de "fichage" d'une société, voire les relations entre ces fichiers, leur concentration, etc.

- C'est également le droit pour chacun de connaître l'existence d'informations le concernant dans un fichier. On a beaucoup glosé sur cette faculté du droit d'accès. Les partisans de la vie privée réclamant que notification soit faite obligatoirement par les ficheurs lors du premier enregistrement sur une personne, les entreprises et les administrations répliquant par le coût d'une telle mesure. On notera que dans tous les projets, le système de la notification obligatoire n'est retenu que pour certains types de fichiers.

- Le corollaire du droit que nous venons d'évoquer est le droit pour le fiché de connaître non seulement qu'il est fiché, mais bien comment il est fiché, en d'autres termes,

quelles informations sont reprises sur lui ?; à quoi et à qui servent-t-elles ? Toutes les expériences étrangères démontrent que les fichés utilisent peu ce droit. A ce propos, on note la réflexion de la CNIL française (second rapport) : "La Commission est parfaitement consciente que quels que soient les moyens qu'elle puisse mettre en oeuvre, le contrôle de l'utilisation de l'informatique nominative ne deviendra vraiment effectif que le jour où il sera exercé par les intéressés eux-mêmes, c'est-à-dire les personnes fichées". La survie de nos libertés dépend de chacun de nous.

On note l'application que certains droits (suédois, français, luxembourgeois) ont tiré de cette facette du droit à l'information et ce à propos des fichiers publics en consacrant le principe du *libre accès des personnes aux dossiers administratifs*. L'informatique permettrait non seulement d'améliorer la qualité du service public mais également d'instaurer un dialogue administré-administration. Ceci nous amène à une réflexion plus générale. L'informatique permettant aux entreprises et à l'administration de décharger leur personnel de certaines tâches répétitives, la réglementation ne doit-elle pas exiger de ces entreprises et de cette administration qu'elle réaffecte son personnel à des tâches d'accueil et de dialogue avec les usagers ?

- Cette idée que je viens d'exprimer se traduit également dans le fait que la plupart des législations, en cas de contestation par le fiché de la qualité des données ou de la pertinence de l'utilisation de celles-ci, exige que dans une phase précontentieuse, le ficheur entende les récriminations du fiché.

Ce n'est qu'au terme de cette phase précontentieuse et à défaut d'accord que le fiché saisira les tribunaux. A ce propos, je ne puis suivre la plupart des projets belges qui, au nom du respect de la vie privée des fichés, exigent un procès en chambre du conseil ou devant un organe particulier ayant des compétences juridictionnelles. Il m'apparaît au contraire que c'est aux juridictions classiques que doit être réservé en principe le soin de trancher au terme d'un débat public les questions du droit à l'information des ficheurs et de ses limites. Une fois encore, c'est toute la problématique négative : "Informatique et vie privée" qui est remise en question. Quelques brèves remarques sur le rôle du troisième personnage, l'autorité de contrôle achèvent de démontrer la nécessité de sortir de ce débat.

3. L'AUTORITE DE CONTROLE

En effet, les questions du statut et du rôle de l'autorité de contrôle révèlent à l'évidence que la réglementation de l'informatique a d'autres enjeux que la seule défense de notre vie privée. Mieux, son expérience dans les pays voisins témoigne de l'apparition de nouveaux enjeux encore, nouveaux enjeux qui conduisent à faire éclater définitivement l'interrogation classique que l'homme de la rue pose devant le développement de l'informatique, en termes de "vie privée" ou de jardin clos à défendre.

Un rappel de l'historique de la création de la CNIL suffira à illustrer le fait déjà énoncé que l'informatisation renforce l'exécutif et qu'il est nécessaire de renforcer les autres pouvoirs constitutionnels afin de rétablir leur équilibre, garantie de nos libertés publiques.

Le rapport préalable TRICOT avait conseillé que la Commission comprenne des Parlementaires mais le projet gouvernemental avait préféré ne pas tenir compte de cet avis et, tout en faisant une autorité administrative indépendante, avait accentué le contrôle de l'Exécutif. La discipline de vote à l'Assemblée nationale n'avait pas permis que la proposition TRICOT trouve écho dans un amendement. Le Ministre Garde des Sceaux évoqua même par après au Sénat "la lourdeur de la tâche de la Commission et son indignité pour les Parlementaires". Et ce n'est que devant la pression massive du Sénat que le Gouvernement céda et obligea sa majorité à l'Assemblée à revenir sur ses votes précédents. Cette présence de Parlementaires dans la Commission (ils sont quatre sur les 17 membres) a valeur de symbole plus que de décision; c'est en quelque sorte l'opinion publique qui veut pénétrer les secrets du monde de l'informatique et se protéger contre l'arbitraire de l'Exécutif.

Mais le débat soulevé par l'informatisation du secteur public n'est pas seulement celui de l'équilibre entre pouvoirs législatif et exécutif, c'est également celui de l'équilibre à maintenir entre les pouvoirs centraux, régionaux et locaux.

Ainsi, il importe que l'autorité de contrôle reste indépendante et ne puisse en aucune manière se confondre avec le contrôlé, au premier chef, l'exécutif. Son rôle est de garantir les libertés et d'empêcher qu'une circulation trop fluide de données nominatives que ce soit dans le secteur public ou dans le secteur privé ne confère au détenteur de ces informations des pouvoirs excessifs que ce soit sur des administrés ou sur des clients. Il ne s'agit pas non plus pour cette autorité de devenir *juge et censeur*, mais de jouer à plein le rôle d'ombudsman, ayant

à la fois pour tâche d'aider individuellement les personnes à défendre leurs droits auprès des tribunaux traditionnels mais également pour devoir de rendre compte au public, et en particulier, au législateur des problèmes de société soulevés par l'informatisation, c'est-à-dire d'aider à la transparence. Cette autorité doit être créée chez nous, nonobstant tout argument budgétaire.

Elle est, en effet, une pièce maîtresse du dialogue à instaurer entre ficheur et fiché pour la définition d'un "modus vivendi" respectueux à la fois du droit à l'information des uns et des libertés des autres et cherche à créer une informatique que certains commentateurs du célèbre rapport NORA-MINC qualifient de "conviviale", dans la mesure où elle remet en valeur le contrôle des hommes et de leurs institutions sur les outils de leur propre création.

Cette tâche de l'organe de contrôle l'a amené à apercevoir de nouveaux enjeux que ceux aperçus jusqu'ici (à savoir le respect des libertés individuelles économiques et publiques). Ces nouveaux enjeux sont les risques créés pour les libertés collectives du travail de l'expression pour la liberté de l'Etat ensuite.

1. Ainsi le CNIL (second rapport) a créé en son sein une sous-commission "Informatique et libertés du travail". Cette sous-commission est notamment chargée de suivre les expériences d'approche participative de l'informatisation des entreprises. On sait que l'informatisation des entreprises pose des problèmes d'emploi et de réallocation des tâches et du temps de travail. Ne faut-il pas, comme en Allemagne, permettre une codécision entre travailleurs et entrepreneurs sur l'informatisation progressive de l'entreprise ? A ce propos, on signalera l'exemple de l'administration Berlinoise qui a signé une Convention avec les représentants des travailleurs et des administrés sur l'informatisation des services communaux. Cet exemple m'apparaît significatif d'une volonté à peine naissante chez chaque homme de savoir et discuter ce que l'informatique va lui apporter comme style de vie.

2. De même, le développement de la télématique a amené la création à la CNIL (second rapport) d'une seconde sous-commission. Il s'agit pour cette sous-commission "de préserver, je cite, la diversification des moyens d'information à la fois par une spécialisation et par l'expression des tendances idéologiques multiples où chaque citoyen pourrait trouver et choisir ce qu'il préfère", cette tâche ne peut être réalisée comme le démontre bien l'expérience Prestel que par une concertation indispensable entre tous

les acteurs c'est-à-dire les consommateurs, les organisations représentatives de ceux-ci, les organes de presse de tout bord, etc.

3. Enfin, les flux transfrontières suscitent des inquiétudes d'un ordre supérieur encore. S'il faut maintenir le principe de la liberté là aussi, il est peut-être bon que ce principe soit assorti de garanties quant au respect de la liberté de chaque Etat. Comme le note MADEC, "le développement actuel des flux transfrontières de données consacre et amplifie *l'ascendant que prennent aujourd'hui les systèmes multinationaux sur les Etats*. Certes, le fait national demeure très vigoureux. Mais il risque de se vider peu à peu de son contenu."

"La simple possibilité de mettre en oeuvre une politique nationale indépendante serait remise en question : déjà, les filiales de multinationales étrangères s'intègrent difficilement dans une politique industrielle; le volume des trésoreries libres consolidées interdit le retour à des parités fixes; la facilité de transférer les cash-flows, grâce à l'anarchie comptable des flux informationnels, met au défi le principe de territorialité fiscale. Aujourd'hui, la téléinformatique permet de faire naître les bénéfices pétroliers ou les eurodollars n'importe où, sur quelque ordinateur-hôte situé dans quelque micro-Etat "compréhensif". La totale liberté des flux transfrontières porte en germe le dépérissement des Etats-Nations".

De même, le principe de l'indépendance de chaque Etat apparaît bien faible lorsqu'il se révèle comme en Suède, que plus de 50 % des informations relatives à la défense du pays sont traitées dans un centre californien ? Dans ce pays, la proportion est bien plus importante dans le domaine des données économiques et on imagine qu'elle voisine les 100 %, pour la plupart des pays en voie de développement.

"Que la panne du "réseau télématique" porte demain sur l'interruption des flux, la cessation des traitements ou l'altération des fichiers et des logiciels et que la cause soit une défaillance technique, une catastrophe naturelle ou une intervention humaine (sabotage, terrorisme, crise politique), l'Etat qui aura transféré des données à l'étranger, à son insu le plus souvent, sera privé de tout argument de souveraineté pour définir une solution du problème. La seule voie est ici de garantir dans le droit international la continuité des flux et la détermination des Etats à refuser la constitution de "paradis de données", que ceux-ci soient motivés par la discrétion ou par la complaisance des pouvoirs publics locaux".

Des solutions législatives existent dans certains pays. On citera à ce propos, la loi française du 16 juillet 1980 sur la communication des documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères tend à prévenir les atteintes à la souveraineté, à la sécurité et aux intérêts économiques de la France et des Français qui pourraient résulter de certains flux sortants d'informations.

Plus intéressantes encore, ces recommandations de la conférence de l'IBI, conférence tenue dans le cadre de l'UNESCO au mois de novembre 1979 qui transposent au plan des Etats certaines notions dégagées par les réglementations locales au plan individuel : droit d'accès, droit de correction, etc... "Tout Etat jouit du privilège d'accès à l'information détenue sur ses réalités ou activités nationales à l'étranger".
"Lors du traitement d'un dossier présenté par un pays, un organisme international ne peut se référer qu'aux seules données émanant du pays intéressé, à l'exclusion des données de toute autre source ...".

Cette référence au principe du droit à l'image qui fonde le droit à l'information des individus témoigne que la question posée par l'informatisation, qu'elle se place au niveau des libertés des individus, des entreprises, des collectivités voire des états, est fondamentalement la même. Le danger le plus réel que notre société encourt par rapport à l'informatique n'est pas à situer du côté d'une infraction à la vie privée des personnes mais plutôt du côté de l'appropriation du pouvoir sous couvert d'une gestion orientée vers le service à rendre, par des groupes difficilement contrôlables et échappant au jeu des instances régulatrices.

Face à ce danger, les individus, les entreprises, les collectivités et les états désirent se réapproprier leurs libertés, c'est-à-dire la liberté de participer à la définition du type de société dans lequel ils pourraient s'épanouir.

En conséquence et conclusion, Mesdames, Mesdemoiselles, Messieurs, je crois qu'il y a deux malentendus à éviter :

1. *"Ne pas se tromper de plan.* Le problème "Informatique et libertés" pose foncièrement non pas une question d'informatique, ni davantage une question de droit. Un texte ne peut servir que si les mentalités changent; d'où le besoin d'informer, de se grouper à la base, d'agir

de façon concertée. Il s'agit en soulevant le problème de l'informatique et de nos libertés de mettre en cause la conception de l'administration, du service public et finalement de la société. C'est à ce propos que doit se focaliser notre attention. L'ordinateur, technique servante, ne peut se substituer au changement de fond. Evitons donc de croire qu'on a changé les choses en profondeur parce qu'on a légiféré. Evitons, à l'inverse, de croire que rien n'a changé tant que, comme en Belgique, il n'y a pas de dispositions réglementaires. Les mentalités ont changé, changent, et c'est heureux. Se prennent, en dehors de l'enceinte parlementaire des orientations qui vont limiter et orienter nos choix de sociétés. Une prise de position législative ne changera rien à ce fait".

2. *"Ne pas se tromper de cible.* Protéger le citoyen, ce n'est pas seulement protéger sa vie privée, mais c'est surtout aménager la relation de pouvoirs, entre personnes d'abord, entre individus, et autorité(s() publique(s) ensuite. Au droit négatif d'être laissé seul, au droit à l'oubli, se substituent peu à peu le droit d'être soi-même, le droit de disposer d'un pouvoir personnel et d'en négocier l'exercice dans sa relation avec la puissance d'autrui (publique ou non). L'exercice de ces droits, l'aménagement de cette relation, l'informatique peut les compromettre ou les aider". (Conclusions de l'atelier nr. 7, Journées Informatique et Société).

L'informatique est comme la langue d'Esope ni bonne ni mauvaise. Elle est ce que nous en ferons ensemble.

BIBLIOGRAPHIE

Banques de données, Entreprises - Vie privée, Actes du Colloque de Namur, 25-26 septembre 1979, Bruxelles, CREADIF, 1980.

Commission Nationale Informatique et Libertés (CNIL), 1er, 2ème, 3ème rapport d'activité, La documentation française.

Une société informatisée : Pour qui, Pour quoi ? Comment ?, Namur, colloque des 21-23 mai 1982, Namur, Pun, 1982, nr. 7 et 7bis.

MADEC, A., "Les flux transfrontières de données : vers une économie internationale de l'information", La documentation française, 1981.

BURKERT, H., "Institutions of Data Protection", Computer Law Journal, 1982, 167 et s.