Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Le fondement du droit à la protection des données nominatives

Poullet, Yves

Published in:
Nouvelles technologies et propriété. Actes du colloque tenu à la Faculté de droit de l'Université de Montréal, les 9 et 10 novembre 1989

Publication date:
1991

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 1991, Le fondement du droit à la protection des données nominatives: "propriété ou libertés". Dans *Nouvelles technologies et propriété. Actes du colloque tenu à la Faculté de droit de l'Université de Montréal, les 9 et 10 novembre 1989.* Litec, Paris, p. 175-205.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 24. Apr. 2024

6131

LE FONDEMENT DU DROIT A LA PROTECTION DES DONNEES NOMINATIVES :

"PROPRIETE OU LIBERTES"

Yves POULLET,
Professeur à la Faculté de Droit
de Namur
Directeur du Centre de Recherches
Informatique et Droit (C.R.I.D.) des
Facultés de Namur

Colloque de Montréal

Novembre 1989.

1. La question du fondement du droit à la protection des données peut-elle éclairer à la fois le contenu de ce droit, ses limites et son mode original de réglementation ?

Les organisateurs du colloque suggèrent le "droit de propriété" ou, plus largement, le "droit réel" comme figure explicative des prérogatives que les réglementations de protection des données accordent dans nos pays d'Europe occidentale à l'individu sur son "image informatisée".

Notre propos abordera donc comme première thèse, celle suggérée par les organisateurs . Le droit réel se définit comme un droit subjectif de la personne. Il se caractérise par une prérogative directe et immédiate sur le bien, en l'espèce immatériel : la donnée, objet de ce droit. Il impose à tous un devoir d'abstention, né de l'obligation de respecter cette prérogative. Ces différentes caractéristiques du droit réel ne justifient-elles pas les attributs reconnus à celui que l'on pourrait considérer dès lors comme le "propriétaire" de l'information nominative. La notion, souvent évoquée, de "vie privée", c'est-à-dire de "vie qui nous appartiendrait", par opposition à celle de vie publique, ne consacre-t-elle ce droit de propriété comme fondement du droit à la protection des données de cette vie privée.

L'analyse de la première thèse nous aménera à une seconde proposition : le débat autour de la vie privée n'obscurait-il pas un autre débat bien plus riche et plus large : celui des libertés individuelles. La notion de liberté conçue comme une maîtrise exercée par le sujet sur lui-même (das sebstbestimmungsrecht), nous apparaît mieux à même d'élucider les débats et solutions actuels en matière de protection des données.

PARTIE I : LE DROIT REEL COMME FONDEMENT EXPLICATIF DU DROIT A LA PROTECTION DES DONNEES

2. Dans un article célèbre, CATALA écrit : "(La législation de protection des données) reconnaît aux individus des prérogatives considérables sur les données qui les concernent nommément, les droits d'accès et de rectification en particulier. La même loi ouvre aux personnes la faculté de s'opposer, pour des raisons légitimes, à leur inclusion dans un fichier nominatif; elle leur donne, enfin, le droit d'exiger des renseignements de celui qui recueille l'information : intéressante innovation, empruntée aux procédés de défense du consommateur, mais qui protège ici le fournisseur. Ce sont là des prérogatives du droit réel. Elles consacrent implicitement l'appartenance de la donnée nominative à la personne concernée, légitime titulaire qui peut, en cette qualité, vérifier leur bon usage et leur véracité". L'auteur poursuit : "Il nous paraît donc que la protection accordée aux individus par la loi sur l'informatique et les libertés reflète un droit sur l'information personnalisée plutôt qu'un droit à cette information" et conclut : "Il ne suffit pas d'affirmer le droit d'un sujet sur un objet immatériel pour en assurer efficacement la sauvegarde, en l'absence d'une législation spécifique attribuant au titulaire du droit des prérogatives adaptées à cet objet et inspirées de l'opposabilité absolue".

Ainsi, selon CATALA, le droit à la protection des données nominatives se construit sur un schéma comparable à celui des droits subjectifs réels. Caricaturant le raisonnement, on affirmera :
1. que l'individu est titulaire d'une relation privilégiée aux données nominatives le concernant;
2. que ces données constituent un objet immatériel, comme une oeuvre d'art peut l'être;
3. que la relation à cette information, à cette donnée nominative, est opposable à tous, soit -et l'analogie se poursuit- qu'il s'agisse d'un droit réel absolu, exclusif comparable à la propriété dans les cas où le sujet de droit peut refuser la divulgation de certaines données minimales le concernant (infra n° 3); soit qu'il s'agisse, pour les autres données, d'un droit réel "démembré", dans la mesure où l'exercice par autrui d'un droit de propriété sur

l'information nominative est limitée par certaines prérogatives du fiché comme le droit d'accès, de rectification voire, à noter l'analogie avec la terminologie en usage en matière de droit réel, de suite.

A. Les "données interdites" comme conséquence du droit de propriété de l'individu sur certaines données le concernant

a. La thèse

3. La première définition du droit à la vie privée, le "right to be let alone" de WARREN et BRANDEIS (1870), accrédite la comparaison entre ce droit et le droit de propriété. La vie privée se définit d'abord comme une liste de données qui en soi objectivement relèveraient du domaine de l'intimité et sur lesquelles dès lors aucun enregistrement ne pourrait avoir lieu. La Convention du Conseil de l'Europe les énumère :

Art. 6 : les données à caractère personnel révélent l'origine sociale, les opinons politiques, les convictions religieuses ou autres convictions ainsi que les données à caratère personnel relatives à la santé ou à la vie sexuelle, données à caractère personnel concernant des condamnations pénales (à moins que le droit interne ...)

La liste de ces données, élargie dans certains pays, dessine autour de l'individu un enclos protégé des regards d'autrui, un jardin de Candide, l'individu ayant seul le droit "sur" de telles données, émanation de sa personnalité objectivée. Cette propriété exclusive lui permet de s'opposer à tout partage des données avec autrui.

"La vie privée", écrit RAVANAS, "est pour l'individu une sphère secrète de la vie d'où il a le pouvoir d'écarter les tiers".

Dans d'autres hypothèses, le partage de la propriété d'une donnée nominative avec un tiers est permis mais soumis à un consentement exprès de la personne, titulaire de la données. Le modèle juirique de l'échange, c'est-à-dire de la transmission par l'individu d'une données le concernant, ainsi celle relative au passé judiciaire, en contrepartie d'un service attendu du ficheur, par exemple, le service attaché au compte bancaire donné par la banque, justifierait de telles dispositions.

b. La réfutation

4. L'idée du droit de propriété comme fondement explicatif d'un droit de l'individu sur certaines données le concernant ne résiste pas à l'analyse.

Premièrement, le droit de propriété se définit d'abord et avant tout par la possibilité de disposer d'un bien. La notion de "données interdites" exclut précisément toute disposition de ces biens immatériels.

Secondement, certaines "données interdites" présentées comme le noyau dur de la vie privée. Ainsi, la race, les opinions syndicales, philosophiques et religieuses peuvent être publiques. Qui peut cacher sa race, le militant syndical ou le prêtre entendent-ils taire leurs appartenance ? A y regarder de près, ce n'est pas tant la vie privée, concept flou indéfinissable qui justifie l'interdiction de traiter, voire de collecter, de telles données que la crainte a priori que l'objectivation en une telle donnée de la personnalité de quelqu'un n'augmente, traitement informatique aidant, le risque de discrimination vis-à-vis de telles personnes.

5. En d'autres termes, c'est la protection des libertés inaliénables de la personnalité, celles d'exprimer ses opinions tant philosophiques que religieuses, celle d'appartenir à un syndicat, celle de mener sa vie sexuelle comme on l'entend et non la protection de la vie privée conçue comme l'envers d'une vie publique qui justifie le traitement particulier de certaines données de la personnalité.

Un tel fondement relativise la notion de données sensibles. Elles ne sont pas sensibles en soi, c'est-à-dire comme noyau dur d'une vie privée dont je serai propriétaire, mais bien dans la mesure où le traitement a priori fait peser un risque de discrimination. ainsi, avec SIMITIS, admettra-t-on que la liste des données interdites ne peut être indéfiniment élargie et surtout que l'intérêt général ou la liberté d'autrui puissent justifier des dérogations, qu'enfin, l'interdiction puisse être levée si la personne, en tout connaissance de cause et en pleine liberté, accepte qu'autrui traite telle donnée a priori sensible.

6. Une dernière réflexion en même temps qu'elle achève notre critique du premier fondement du droit à la protection des données, conforte notre conviction de la nécessité de glisser du débat "Informatique et vie privée" à celui "Informatique et libertés", dont au passage on notera qu'il est le titre même de la loi française du 6 janvier 1978. CATALA cite à l'appui de sa thèse, l'article 26 de cette loi qui autorise la personne, titulaire de données, à s'opposer, pour des raisons légitimes, à leur inclusion dans un fichier nominatif.

La CNIL, dans son rapport sur dix ans de fonctionnement, note que ce droit constitue la manifestation la plus éclatante et la plus tangible d'un droit de maîtrise et de contrôle de l'individu sur les informations qui le concernent.

Le droit de propriété n'est-il pas, dès lors, affirmé lorsqu'on reconnaît à quelqu'un le droit de s'opposer à toute utilisation par un tiers de son bien ? Deux réflexions nous amènent à nuancer fortement cette affirmation :

- la disposition française est exceptionnelle, nous n'avons pas trouvé, dans aucune autre législation, de consécration de ce droit de s'opposer a priori à une prise de renseignements. Certes, le droit à l'information du tiers peut être fortement limité (respect du principe de finalité, non communication à des tiers, etc.) mais en aucune manière, il n'est affirmé dans d'autres pays, la priorité du droit de l'individu sur l'information le concernant par rapport au droit des tiers à pouvoir traiter cette information;

- la disposition française ne consacre pas d'un droit absolu mais d'un droit fonctionnel, c'est-à-dire limité par sa finalité, l'intérêt légitime de la personnalité du fiché. Le rapport de la CNIL, déjà cité, commente comme suite ce passage : "Les raisons légitimes n'étant pas définies a priori par la loi, leur reconnaissance reste soumise, au cas par cas, à l'appréciation des tribunaux", et ajoute : "Pour nombre de traitements du secteur public, ce droit n'existe pas".

7. Certes aucune jurisprudence n'est encore venue interprêter l'article 26 de la loi française. Mais à y regarder de près, celui-ci ne consacre pas une prérogative directe et immédiate de l'individu sur telle ou telle donnée mais bien, dans une situation particulière où la prise d'une information mettrait en danger la liberté de celui sur lequel cette information porte la possibilité, pour ce dernier, de faire valoir son intérêt légitime à limiter le droit à l'information du tiers. Le juge aura alors à mettre en balance deux intérêts, celui de l'intéressé à ne pas voir traiter la donnée le concernant et ce au nom du danger que représente le traitement pour ses libertés et celui du ficheur, à traiter la donnée au nom également de sa liberté qu'on l'appelle liberté d'entreprendre ou autrement.

En d'autres termes, l'article 26 invite à une réflexion bien plus fondamentale que celle d'une vie privée introuvable. Elle conduit à entrevoir la nécessité dans ce débat sur la protection des données, d'un arbitrage entre libertés s'opposant dans un contexte donné. C'est là le sens de notre seconde thèse (cf. infra, n° 14 et s.).

B. Les droits réels ou de propriété intellectuelle comme explication des droits de l'individu sur la donnée détenue par les tiers.

a. La thèse

8. Si l'idée d'un droit de propriété sur les données ne peut résister à l'analyse, tout au moins faut-il reconnaître, selon certains, que les prérogatives accordées par les législations de protection des données à la personne enregistrée s'apparentent curieusement à celles qui caractérisent les droits réels ou de propriété intellectuelle. Leur caractéristique commune est en effet la consécration d'un droit direct et immédiat portant sur un bien et opposable à tout tiers, y compris au propriétaire de ce bien.

L'auteur d'une oeuvre littéraire et artistique peut, au-delà de la cession de son oeuvre, précisément au nom de son droit de propriété intellectuelle, s'opposer à toute déformation de l'émanation de sa personnalité, à une reproduction infidèle ou non autorisée de son oeuvre et ne voit-on pas consacrer les mêmes principes dans les législations de protection des données lorsque celles-ci reconnaissent à la personne fichée, par le droit d'accès, le droit de contrôler le caractère exact, à jour et complet, des informations et ce lors du stockage, du traitement et de la transmission de ces informations, par le droit de suite (à noter l'appellation empruntée de la terminologie du droit réel), le droit de suivre la donnée litigieuse en quelques mains où elle se trouve pour en exiger le cas échéant la correction et par le principe de pertinence, celui de contrôler le respect de la destination de la collecte de la donnée.

9. Le parallèle séduisant entre les droits réels ou de propriété intellectuelle et ceux déduits des législations de protection des données repose sur le principe de base identique à celui évoqué dans notre analyse du droit de propriété comme fondement du droit à la vie privée : il existerait une relation immédiate et directe entre l'individu et la donnée le concernant, en d'autres termes, le raisonnement commence dans le premier temps par objectiver la notion de donnée personnelle, ce qui, en réalité, n'est jamais qu'un prolongement de ma personnalité et comme tel est non détachable de moi, pour lui attribuer, dans un second temps, un ou plusieurs titulaires qui se partageraient les droits sur cette information. Ainsi, la banque qui collecte des informations et les inscrit sur la carte à mémoire permettant ainsi l'accès à certains services bancaires pourrait être dite propriétaire de telles informations à charge de respecter les droits réels de la personne, objet de l'enregistrement.

b. La réfutation

10. La comparaison peut facilement être réfutée et son analyse nous invite à emprunter une voie qui précisément quitte le domaine des droits subjectifs réels ou assimilés pour rejoindre celui des droits de la personnalité ou des libertés.

Le droit pour le fiché d'exiger vis à vis du ficheur la non modification de la donnée nominative, sa correction, le respect de sa destination ressemble étrangement aux prérogatives que le droit moral (qualifié encore de droit extrapatrimonial) confère à l'artiste sur son oeuvre. "Le droit moral, nous dit la cour de cassation française (Cass. 6 juillet 1965, G.P., 1965, 2, 126) qui appartient à l'auteur d'une oeuvre artistique donne à celui-ci la faculté de veiller après sa divulgation au public, à ce que son oeuvre ne soit pas dénaturée ou mutilée (cf. dans le sens, la jurisprudence allemande du Reichsgericht, RGZ, 79, 397, 399). L'analogie des droits du fiché avec la catégorie des droits extrapatrimoniaux incessibles, strictement personnels et inaliénables plutôt qu'avec celle des droits patrimoniaux se justifie aisément. Les législations de protection des données insistent sur le caractère personnel du droit d'accès, interdisent toute cession de celui-ci voire l'exercice collectif du droit et certaines législations (Cf. à cet égard, l'avant-projet belge) punissent sévèrement l'extorsion des données par un tiers contraignant le titulaire du droit d'accès à l'exercice de ce droit d'accès.

Sur la donnée nominative comme sur l'oeuvre d'art, se superposeraient donc deux droits également absolus et universellement opposables,celui patrimonial du propriétaire du fichier,du produit informationnel dans lequel s'incorpore la donnée nominative, et celui ,extra patrimonial ,du fiché.

11. La jurisprudence s'est parfois penchée sur les rapports qu'entretiennent le droit moral de l'auteur et les droits patrimoniaux sur l'oeuvre d'art, exercés par autrui. Ainsi, dans l'arrêt Lecocq, compositeur de musique du début du siècle, la Cour de Cassation (Cass. 25 juin 1902, D.P., 1903, I, 5, note A. Colin) distingue clairement l'exploitation économique,attribut du droit d'auteur et le droit moral,autre attribut de ce droit d'auteur. En l'occurrence, les droits patrimoniaux d'exploitation économique appartenaient à la communauté des biens et formaient la copropriété des époux Lecocq dissoute depuis par le divorce de l'auteur mais,selon la Cour,cette mise en commun du monopole d'exploitation a lieu sans qu'elle puisse porter atteinte à la faculté de l'auteur inhérente à sa personnalité même, de faire ultérieurement subir des modifications à la création, ou même de la supprimer, pourvu qu'il n'agisse pas dans un but de vexation à l'égard de son conjoint.

12. Parmi les prérogatives du droit moral de l'auteur, la doctrine en distingue deux types. Le premier s'attache à des prérogatives ayant un contenu précis, tel le droit à la paternité: chaque auteur peut réclamer de voir son nom figurer sur l'oeuvre dont il est l'auteur ,une telle prérogative étant comme telle opposable à quiconque . Le second type de prérogatives n'a pas ce contenu précis,ainsi le droit au retrait,à la non déformation de l'oeuvre ne peuvent s'excercer de façon aussi absolue mais le bien fondé de leur excercice dépendra d'une appréciation du juge mettant en balance la gravité de l'atteinte à la personnalité de l'auteur,d'une part,et le droit d'autrui ,d'autre part : de telles prérogatives ne sont pas absolues, elles peuvent entrer en conflit avec celles issues d'autres droits, le propriétaire de l'oeuvre d'art peut décider de la détruire ou de l'exploiter de telle ou telle manière,l'auteur ne pourra invoquer l'atteinte à sa personnalité que dans des cas rares où le mode concret d'exploitation ne correspond manifestement pas à la pensée manifestée de son auteur (l'auteur connu pour ses idées pacifistes dont la création sert à la publicité d'armes de guerre).Autre exemple, il est clair que le principe de l'inviolabilité du domicile s'opposera à ce que l'auteur puisse contrôler le respect dû à son oeuvre au domicile du propriétaire (Paris 6 juillet 1975, G.P., 1965, 2, 126). Dans l'affaire Lecocq, le juge vérifie si l'exercice du droit de la personnalité ne représente pas un abus de droit lorsque l'auteur s'oppose à l'exercice légitime par autrui des droits patrimoniaux ou d'un droit de propriété sur l'oeuvre d'art.

En conclusion, comme le note Rigaux (T.II, p. 178) à propos de ces particularités et conflits, "il est contradictoire de reconnaître à deux personnes, une prérogative construite sur le modèle du droit de propriété en attribuant à l'une et à l'autre, la maîtrise d'un droit dont il appartient à chacun de déterminer, comme il l'entend, l'étendue". En réalité, il s'agit de deux prérogatives de nature différente, l'une relève des biens de la personnalité, selon l'expression du même auteur, l'autre des droits civils patrimoniaux.

Conclusions.

13. Au vu des considérations qui précèdent, la thèse du droit de propriété ou des droits réels comme fondement justificatif des législations sur la protection des données nous apparaît à la fois **erronnée, dangereuse et incapable** d'expliquer l'évolution du débat de la protection des données.

Chaque terme de la proposition est justifié comme suit:

- la thèse est fausse dans la mesure où elle prétend isoler la donnée de son contexte pour la définir comme objet d'un droit réel. Or même pour les données sensibles, les législations de protection des données ne reconnaissent pas une valeur aux données en soi mais les envisagent dans leur contexte fonctionnel, c'est-à-dire en considération des finalités de leur enregistrement ou de leur traitement. A cet égard, les législations de protection des données entendent d'abord et avant tout contrôler la nature et le droit à l'information des ficheurs plutôt que reconnaître a priori un lien direct entre la personne et la donnée la concernant.

- la thèse est dangereuse, situant le droit à la protection sur le terrain des droits réels elle induit l'idée d'une commercialisation possible de ce droit (Rodota). A cet égard, le débat américain sur la règlementation des câbles de télédistribution est exemplaire. En 1982, le président de la F.C.C., dans une étude intitulée : "Economics and Privacy in Telecommunications", justifie l'inutilité de toute règlementation spécifique "Privacy" à propos de l'enregistrement des données d'utilisation du câble (le choix des programmes de télévision, la durée de l'écoute), en affirmant que la concurrence dans ce secteur amènerait les opérateurs soit à offrir à ceux qui le désireraient contre paiement les garanties de confidentialité requise, soit à se distinguer de cette manière. En d'autres termes, selon Possner, la "privacy" pourrait comme tout autre bien marchandable s'acheter ou du moins se négocier.

Les adversaires de cette position (Gardner and White, Westin) notèrent que:

+ les règles du jeu ne peuvent jouer là où il existe une telle distorsion entre les pouvoirs des parties supposées contractantes potentielles;

+ le débat dépasse la question d'une libre disposition d'un soi-disant bien patrimonial pour rejoindre celle d'un débat public sur la protection d'une liberté publique essentielle, la liberté d'opinion , en l'occurrence révelée par le choix d'émissions télévisées.

-la thèse, enfin, est incapable de rendre compte des évolutions règlementaires. Ainsi, le droit au consentement libre et éclairé préconisé par des règlementations nouvelles suscitées par des nouveautés technologiques comme le R.N.I.S. ou les cartes à mémoire ne se justifie pas par l'existence de nouvelles données mais bien dans la mesure où l'évolution du fait technologique crée de nouvelles formes de circulation de l'information appelant des garanties supplémentaires pour les libertés des citoyens.

En d'autres termes, pour reprendre les conclusions de l'IBI,"maintes fois, il a été proposé et discuté la comparaison entre le droit à la confidentialité dans la vie privée,invoquée par l'homme dans notre siècle et le droit de propriété privée, proclamé comme un "droit naturel "dans les siècles précédents,et duquel on pourrait rtapprocher le "right to privacy tels que l'entendaient ses premiers auteurs,Warren et Brandeis. Certes,il s'agit d'une analogie suggestive mais qui ne peut établir un parallélisme précis... . Dans les conditions de la société actuelle,il concerne plutôt la sphère des droits politiques excercés par le citoyen vis à vis du pouvoir public (et nous ajoutons privé), qui est devenu "pouvoir informatique" en tant que détenteur et administrateur des archives électroniques

les plus complexes... . Il s'agit donc d'une question de liberté, non pas d'une liberté aristocratique qui convient à quelques privilégiés désireux d'être laissés tranquilles,mais d'une liberté démocratique qui concerne tous,dans les relations sociales qui ont pris une nouvelle forme comme suite à la civilisation technologique ."

Dès 1974,Rodota écrivait dans le même ordre d'idées : "Ceux qui sont en mesure de comprendre la nature véritable du débat se rendent compte qu'il ne s'articule plus uniquement autour du thème classique de la défense de la vie privée contre les ingérences extérieures,mais que par suite d'une modification importante d'ordre qualitatif,le problème du secret de la vie privée est envisagé dans le contexte des structures actuelles du pouvoir,structures dont l'information constitue en fait une des composantes essentielles. Pour résumer cette évolution,il faut souligner que le droit à une certaine intimité perd constamment du terrain au profit de la possibilité donnée à l'individu d'excercer un contrôle sur la communication des informations qui le concernent ."

Partie II : Les libertés comme fondement explicatif du droit à la Protection des données.

I. La thèse.

A. La décision du Tribunal constitutionnel fédéral allemand sur le recensement démographique.

14. La loi relative au recensement démographique et ses mesures d'exécution furent l'objet d'un recours des "Verts" (parti écologique) au Tribunal constitutionnel de République fédérale d'Allemagne.

Le jugement du 15 décembre 1983 leur donne raison, il ordonne de compléter le programme d'enquête statistique de certaines mesures procédurales et de sécurité et déclare inconstitutionnelle la communication des données collectées. Le fondement de la décision est l'atteinte aux "droits généraux de la personnalité" progressivement dégagée par le tribunal fédéral allemand sur base des articles 1 (1) (intangébilité de la dignité humaine), et 2 (1) (droit à l'épanouissement de la personnalité) de la loi fondamentale allemande. " Le Tribunal fédéral considère le "droit à l'autodétermination en matière d'information" (Informationnelle Selbstbestimmungsrecht) comme partie intégrante des droits généraux de la personne humaine " la valeur et la dignité de la personne humaine agissant librement comme membre d'une société libre sont les principes essentiels de la loi fondamentale". (Burkert, 1985)

15. Ce droit à l'autodétermination, qui est le droit de tout individu à maîtriser l'image qu'il donne de lui même dans la société est particulièrement mis en danger par les possibilités actuelles et futures de traitements automatisés de l'information. Il ne peut cependant s'entendre de façon absolue: l'individu, note la Cour constitutionnelle, n'exerce pas une souveraineté absolue sur les faits le concernant; sa personnalité se développant au sein d'une communauté sociale, il ne peut vivre sans communiquer. L'information, même si elle est nominative, est une représentation de la réalité sociale, qui n'est pas uniquement la propriété de l'individu concerné....La loi fondamentale résoud la dichotomie individu-société en considérant la personne comme une entité liée et insérée dans la société. C'est pourquoi en principe, l'individu doit accepter des restrictions de son "droit à l'autodétermination en matière d'information" et ce, en faveur de l'intérêt général prépondérant".

B. La liberté individuelle,véritable fondement.

16. Ainsi, le droit à l'autodétermination constituerait le véritable fondement de la législation de protection des données. **Mais, en définitive, qu'est ce que ce droit à l'autodétermination sinon une liberté**, selon l'expression de Rigaux (1988,566) ?

La thèse de Rigaux est précisément de démontrer que la protection de la vie privée et au delà des biens de la personnalité se rattache directement à la liberté de l'individu et que toute confusion ou comparaison avec les droits subjectifs patrimoniaux classiques obscurcit le débat. "Devant les biens de la personnalité s'ouvre un champ infiniment plus vaste que celui qui y a été assigné jusqu'ici. Il ne s'agit certes pas de doubler tous les droits patrimoniaux d'un ectoplasme qualifié de droit de la personnalité, mais plutôt de réajuster dans leur ensemble les règles applicables à ces droits d'une manière qui prenne mieux en considération la dignité et la personnalité des agents juridiques privés" (Rigaux, 1988, 578)

Selon l'auteur, le droit à la protection des données ne peut se comprendre en réduisant le débat à la reconnaissance d'un droit subjectif qualifié de droit à la vie privée.

Les droits subjectifs se caractérisent en effet par le fait qu'ils confèrent à leur titulaire l'appartenance maîtrise d'un objet déterminé: "il appartient à la nature de ces droits de conférer à leur titulaire des prérogatives précises accompagnées d'un droit d'exclusivité"(Rigaux, p.575). **"Existe t'il une "sphère privée" qui ferait l'objet d'une appropriation exclusive du sujet et,en tant que telle soustraite à toute immixtion de tiers ? La maîtrise de cette sphère privée est-elle protégéepar un droit subjectif inconditionnel analogue au droit de propriété ? L'impossibilité de circonscrire cette sphère autrement que par une définition tautologique impose de donner à ces questions,une réponse négative . La recherche d'un noyau dur qu'on appellerait "intimité de la vie privée" n'est pas moins vouéee à l'échec . Même les atteintes les plus graves,qu'on peut présumer illicite et qui ont généralement ce caractère le perdent dans des circonstances exceptionnelles . Il arrive que les membres de la société civile aient intérêt à être informés de faits qui appartiennent ...à la vie intime du sujet ou que celui-ci ne puisse se prévaloir d'un intérêt assez contraignant pour résister à pareille divulgation dont l'auteur fait alors un usage qui n'est pas illicite de sa propre liberté ."**

C. Conséquences

17. La thèse de Rigaux met en évidence les points suivants :

a) La liberté et la dignité humaines, fondement ultime des législations de protection des données, justifient eu égard au danger particulier que représente l'usage du traitement automatique des données, la consécration de droits subjectifs précis, permettant aux individus d'avoir les moyens minima d'exercer lers droits à l'autodétermination. La cour constitutionnelle allemande écrit: "Face au danger déjà décrit de l'usage du traitement automatique de l'information, le législateur doit prendre de plus amples mesures qu'auparavant quant à l'organisation et à la procédure d'un traitement de données et ce, afin d'empêcher toute violation du droit de la personne humaine...".Dans cette perspective, serait justifiée la consécration de droits subjectifs particuliers que l'on pourrait rassembler sous la qualification de droit d'accès. L'analogie avec le droit à la paternité,droit subjectif particulier né des attributs non patrimoniaux conférés à l'auteur peut être évoquée à ce propos. Il s'agira de montrer que ce droit subjectif peut prendre de nouvelles formes,eu égard aux dangers nouveaux ou aux particularités de nouvelles techniques

b) La liberté et la dignité humaines affrontent d'autres libertés, celles d'autrui, d'autres intérêts et notamment l'intérêt général.

"Liberté plutôt que droit, le Selbststimmungsrecht doit se concilier avec la liberté également reconnue à tous les autres sujets de droit. Les droits fondamentaux sont parfois en conflit avec les uns et les autres. Enfin et surtout, le Bundesverfassungsgericht n'a pas reconnu au droit à l'épanouissement de la personnalité, une portée absolue. Chaque fois qu'elle l'estime nécessaire, la juridiction constitutionnelle a rappelé que l'individu est une personne insérée dans la société: celle-ci peut, dans l'intérêt général ou pour la présentation des droits d'autrui, imposer aux citoyens des devoirs ou des abstentions qui empêchent leur liberté naturelle." (Rigaux, 1988, 485). Les législations de protection des données entendent définir certains critères qui permettront de préciser ce droit à l'information du ficheur,expression tantôt de sa liberté d'entreprendre, dans le secteur privé, tantôt de son rôle de gardien de l'intérêt général, dans le secteur public.

c) Enfin,la thèse de Rigaux oblige à mettre l'accent sur la nécessité de définir de façon évolutive l'équilibre des intérêts en conflit et d'approfondir le rôle des institutions chargées en premier lieu d'aider à la définition de cet équilibre dans ce contexte évolutif.

Chacun de ces points fait l'objet de commentaires particuliers.

II . Le fondement explicatif reconnu à la protection des données justifie des droits subjectifs nouveaux aux fichés

A. Explication et contenu

18. Rigaux (1988, 558) écrit : " Dans l'Etat social moderne, l'intangibilité de la dignité humaine ne saurait plus être garantie selon le modèle aujourd'hui dépassé de Locke : liberté et propriété . Ces serait trop dire que les droits nouveaux ont été conçus contre la propriété, mais ils excercent une fonction de complément ou de substitut . Pour que le droit de propriété reste tolérable, avec les considérables inégalités qu'il a entretenues, force a été d'instituer tantôt des droits subjectifs nouveaux, tantôt l'illusion de tels droits . "

Le droit d'accès sous ces multiples facettes reconnu au fiché ne peut-il être, dans cette perspective, considéré comme un droit sujectif nouveau c'est à dire comme le complément ou plutôt le corollaire rendant tolérable le surcroît de puissance que confère le traitement automatisé de données à celui qui les détient . La modification d'ordre tant quantitatif que qualitatif de la valeur informationnelle de la donnée nominative, modification obtenue par le traitement informatique de même que la non transparence des circuits d'information exige la reconnaissance pour le fiché de droits subjectifs nouveaux, rassemblés sous le vocable de" droit d'accès" .

19. En résumé le droit d'accès peut se définir 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 . Ce droit ne nécessitait pas la consécration de droits subjectifs particuliers lorsque dans les sociétés traditionnelles, la circulation de l'information nominative pouvait aisément se contrôler. Il en est tout autrement dans nos sociétés actuelles .

Un exemple tiré de la vie quotidienne suffira à le démontrer : jusqu'il y a peu, le paiement au comptant représentait la forme habituelle de paiement . La valeur informationnelle d'un paiement au comptant est quasi nulle et le vendeur sauf s'il connaît l'identité de son acheteur peut difficilement établir une corrélation entre tel individu et telle dépense . En toute hypothèse, l'acheteur identifié peut connaître a priori les personnes (voisins) à qui l'information sera transmise. Dans le cas de l'utilisation d'un terminal point de vente, le paiement acquiert une valeur informationnelle sans commune mesure avec celle relevée pour le paiement au comptant . Ainsi, l'utilisation du terminal renseigne le banquier (tiers à la transaction) sur l'identité non seulement de l'acheteur mais également du commerçant, l'importance de la transaction voire sa nature. Le commerçant obtient une information sur la relation bancaire de son client et sur sa valeur de crédit . L'utilisation de système informatique pour la gestion de telles informations accroît encore leur valeur informationnelle puisque le recoupement des informations primaires obtenues, leurs comparaisons permettront rapidement à leurs détenteurs de se faire une image précise des habitudes de consommation d'un client, de ses déplacements et de l'importance relative de chacune de ses dépenses . "Même les goûts culturels et artistiques par le biais des librairies et des salles de spectacle fréqentées deviennent soudainement transparents. Bref, à travers chaque transaction économique, l'usager d'une carte de crédit révèle à un tiers qui ne lui demande pas son avis, sa personnalité, ses projets et ses dépenses futures compte tenu de sa situation sociale globale" (Lemasson, 1988).

2O. Classiquement,nos législations d'Europe Occidentale ont envisagé le droit d'accès sous de multiples facettes :

-d'abord, lors de la collecte d'informations, c'est le droit pour le fiché de savoir pourquoi on l'interroge, le caractère obligatoire ou non de la réponse,de connaître l'utilisateur et la finalité d'utilisation de l'information ;

-également, le droit pour le public en général de connaître, par l'existence d'un fichier des fichiers, le degré d'informatisation d'une société, les relations entre les fichiers,leurs concentration ,etc.;

-ensuite, encore que nombre de nouvelles législations abandonnent ou restreignent ce droit, le droit pour chaque individu de savoir qu'il est fiché,afin de lui permettre dans un second temps, de connaitre les données de base (et non les données résultat) figurant à son propos dans le fichier informatisé ;

-enfin, il s'agit pour le fiché de pouvoir exiger, par des procédures rapides et le cas échéant avec l'aide de l'autorité chargée de la protection des données,la rectification, l'effacement de certaines données auprès du ficheur voire auprès de tiers en relation avec celui-ci .

B.**Evolution du droit d'accès**

21. Si le droit d'accès est un ensemble de droits subjectifs nouveaux correctifs d'un droit de propriété auquel les nouvelles technologies de l'information donnent un pouvoir que l'on peut craindre excessif, certains développements actuels de ces nouvelles technologies dans la mesure où **ils accentuent encore la non maîtrise par l'individu des circuits d'information** le concernant conduisent certains à compléter par de nouveaux droits subjectifs le droit d'accès tel qu'il avait été consacré par les législations de protection des données. Le progrès technologique crée de nouveaux modes de collecte de l'information, soit plus insidieux parce que moins transparents, soit plus automatiques parce que liés à l'utilisation d'un service télématique, soit enfin plus dangereuxparce que lié à l'utilisation d'un service d'intérêt général comme le téléphone. Deux débats relayés par les autorités de protection des données,l'un surtout allemand à propos des nouveaux compléments au service téléphonique offerts par le R.N.I.S., l'autre en France, à propos des cartes à mémoire utilisées dans le domaine de la santé, illustrent cette évolution du droit d'accès.

22. A propos des nouveaux compléments du service téléphonique, offerts dans le cadre du R.N.I.S., la discussion en R.F.A. a mis en évidence la nécessité de promouvoir une information préalable de l'abonné au service téléphonique afin que celui ci puisse excercer son **consentement** éclairé à diverses options rendues possibles par la technologie du réseau à intégration de services, ainsi l'identification du numéro de l'appelant,la facturation détaillée, la figuration du nom de l'abonné et de ses qualités dans l'annuaire électronique.

Le **droit à la transparence** des circuits d'information consiste essentiellement dans l'obligation pour l'opérateur, pour toute personne intervenant dans l'exécution du service et pour le serveur d'informer l'abonné des enregistrements,traitements, stockages et cessions de données nominatives le concernant, et ce préalablement à leur collecte. Ce droit à la transparence se double d'un droit au **consentement libre et éclairé** de l'abonné à différents stades : lors du prélévement des données nominatives, ce sera le droit de ne pas figurer dans l'annuaire et d'exiger la non divulgation du numéro d'abonné; ce sera également le droit d'exiger ou de refuser l'envoi automatique de facturations détaillées, la non visualisation de son numéro sur le terminal appelé . Enfin, pointe une légitime revendication complémentaire des deux premières, celle du **droit à l'anonymat,** le droit d'exiger que soient mises en oeuvre des techniques (par exemple,les cartes préchargées anonymes) permettant l'utilisation anonyme d'un service d'intérêt général comme le téléphone .

23. La non transparence des cartes à mémoire en incorporant un microprocesseur a suscité, dans le domaine de la santé du moins, certaines recommandations de la CNIL française prises dans le cadre d'expériences de cartes "Santé". Trois principes les éclairent :

- celui du volontariat : patients et médecins ne peuvent être contraints de participer à la mise en oeuvre d'un système informatisé de traitement des données. Aucun avantage ni aucune pénalisation ne peuvent être la conséquence d'un refus de participation;

- celui du consentement libre et éclairé à l'usage de la carte : patients et médecins doivent être clairement informés des finalités et modalités du système, des modes d'inscription ou d'effacement des informations contenues dans la carte à mémoire; des personnes habilitées à lire ces informations et des garanties, droits et recours dont ils disposent;

- celui enfin de l'exclusion de toute discrimination : le principe du libre choix du médecin par le patient et le principe du choix de la pratique médicale ne peuvent être remis en cause d'une manière ou d'une autre.

Ainsi, la création de nouveaux modes de collecte, de dissémination et de conservation de l'information peut élargir la signification du droit d'accès conçu comme toute mesure visant à permettre au fiché de maîtriser les circuits par lesquels transitent l'information le concernant.

III. Le fondement explicatif reconnu à la protection des données justifie à la fois le droit à l'information des ficheurs et ses limites

A. Explication .

24. Puisque l'individu n'est pas propriétaire des données le concernant, ni même titulaire sur elles d'un droit proche d'un droit réel, puisque c'est de façon spontanée que l'individu projette dans la société une certaine image de lui, cette image précisément peut être captée par autrui,rapprochée d'autres informations et prendre ainsi un sens aux yeux de celui qui la traite. Il ne peut être question a priori de nier à autrui,le droit d'utiliser l'image que je donne de moi même. A ma liberté, s'oppose la sienne qu'il s'agisse de la liberté d'association dans le cadre de traitements opérés par un syndicat, de la liberté religieuse dans le cadre de traitements gérés par l'autorité religieuse ou plus fréquemment de la liberté d'entreprendre dans le cas de fichiers d'entreprises. Ce conflit de libertés doit se résoudre par la **méthode de pondération des intérêts** par laquelle l'autorité chargée de trancher le conflit appréciera les intérêts légitimes respectifs propres à chaque partie exprimant sa liberté.

Nous reviendrons sur ce point mais notons d'emblée que nombre de prescrits législatifs prévoyant une exception pour certaines données ou certains traitements s'explique de la sorte . Ainsi, il est facile de justifier que les législations interdisent le traitement de données philosophiques,syndicales ou religieuses, c'est qu'a priori le traitement de telles données met en péril ma liberté du même nom; que toujours à propos de ces mêmes données, les mêmes législations exemptent de cette interdiction précisément les associations religieuses ou syndicales voire la presse, s'explique par la volonté d'affirmer la prééminence de la liberté d'association, de la presse sur les libertés individuelles.

24 bis.Comme on le note à travers ces exemples limités, l'enregistrement de la même donnée nominative sera tantôt interdit, tantôt réglementé, tantôt libre suivant les libertés mises en cause par son enregistrement. Il y a bien débat entre libertés et nécessité d'apprécier au regard des intérêts de la société le poids accordé à chacun d'elles.

En ce qui concerne précisément la liberté d'entreprendre du ficheur, peut-on admettre, au-delà des limites imposées à l'égard de certaines données qui caractérisent de façon immédiate, des libertés constitutionnelles reconnues (liberté d'opinion, de religieion, d'association), qu'une législation définisse en même temps que le droit à l'information du ficheur, les limits de ce droit. Le principe de la liberté du ficheur de collecter des données ne doit-il pas être affirmé en tant que tel quitte à ce qu'a posteriori, certains abus ne soient régéls in casu par le juge. En d'autres termes, une législation de protection des données doit-elle intervenir vis à vis des traitements du secteur privé autrement qu'en prévoyant un droit d'accès (cf. sur ce point,supra n°18 et s.) et notamment réglementer le contenu et les limites des traitements privés ? La réponse à cette question peut être élucidée par l'étude des principes de la réglementation des traitements du secteur public .

25. Le droit de l'autorité publique à collecter les données et à les traiter ne peut s'expliquer par une liberté fondamentale qui justifierait en soi ce droit. La décision du Bundesgerichtshof déjà citée explicite comme suit le bien fondé de ce droit et en tire des conséquences : "Ce "droit à l'autodétermination en matière d'information" comporte certaines restrictions. L'individu n'a pas un droit absolu, c'est-à-dire n'exerce pas une souveraineté absolue sur les "faits" le concernant; sa personnalité se développant au sein d'une communauté sociale, il ne peut vivre sans communiquer. L'information, même si elle est nominative, est une représentation de la réalité sociale qui n'est pas uniquement la propriété de l'individu concerné. Comme la jurisprudence du Tribunal fédéral constitutionnel l'a mis à plusieurs reprises en évidence, la loi fondamentale résoud la dichotomie individu-société en considérant la personne comme une entité liée et insérée dans la société (...). C'est pourquoi, en principe, l'individu doit accepter des restrictions de son "droit à l'autodétermination en matière d'information" et ce, en faveur de l'intérêt général prépondérant". Ces restrictions du droit à l'autodétermination nécessitent cependant un fondement légal conforme à la Constitution et doivent respecter, en outre, les principes de clarté des normes et de proportionnalité. En ce qui concerne le traitement électronique de l'information, cela signifie concrètement : "Face au danger déjà décrit de l'usage du traitement automatique de l'information, le législateur doit prendre de plus amples mesures qu'auparavant quant à l'organisation et à la procédure d'un traitement de données, et ce, afin d'empêcher toute violation du droit de la personne humaine (...)" (BURKERT, 1985).

Le droit à l'information des autorités publiques indispensable pour assurer un service public efficace nécessite le respect de **trois principes,ceux de légalité,de spécialité et de proportionnalité** . Ces trois principes ont la signification suivante :

- **le principe de légalité** exige que toute banque de données soit créée sous le contrôle du législatif, c'est à dire que les principaux éléments de la réglementation soient définis par une loi au sens formel du terme. De façon générale, ce principe implique une certaine coordination et contrôle par le législatif de l'informatisation du secteur public. On note qu' au delà du problème des libertés individuelles ,est également rétabli par là un certain équilibre des pouvoirs. L'utilisation croissante de l'informatisation dans le secteur public renforce en effet les pouvoirs d'action de l'exécutif et modifie l'équilibre des pouvoirs, garant institutionnel de la démocratie. Le rattachement de l'autorité de contrôle de protection des données au législatif et le droit de saisine large accordé au législatif auprès de cette autorité participent de la même idée .

- **le principe de spécialité** exige que le législateur indique avec précision les objectifs de l'utilisation des données nominatives et les destinataires des ou de certaines

des données collectées. Ainsi,chaque autorité administrative ne peut enregistrer des données que dans le cadre de la mission qui lui a été confiée et pour autant que cela lui est nécessaire au regard de l'intérêt général ou de la protection des intérêts des citoyens **(principe de proportionnalité).** Ces deux principes ont pour conséquence qu'au sein des administrations, "il faut veiller à ce que des traitements dont la collecte et l'utilisation poursuivent des finalités différentes ne soient pas interconnectés. Il faut s'assurer ensuite que chaque domaine distinct de l'activité de l'administration reste bien séparé et, ce par une interdiction de communiquer entre ces secteurs d'activité : le pouvoir exécutif devrait ainsi veiller à créer des domaines informationnels cloisonnés... Le principe général de la séparation des pouvoirs serait en conséquence complété par une "séparation des pouvoirs en matière d'information" (Burkert, 1985).

27. La **consécration de principes parallèles** à ceux développés pour le secteur public permettant de restreindre le droit des ficheurs privés est habituelle dans les législations de protection des données d'Europe Occidentale. Elle peut surprendre l'observateur nord américain qui exclut les traitements du secteur privé du champ d'application des législations de protection des données. L'application analogique européenne des normes régissant les rapports entre le citoyen et la puissance publique s'explique par le fait que l'Etat déborde son rôle constitutionnel traditionnel : "à son devoir traditionnel d'abstention, simplement accompagné de l'obligation générale de maintien de l'ordre, s'ajoute désormais le devoir de prendre les mesures requises pour la sauvegarde des droits fondamentaux auxquels appartient aussi une réglementation satisfaisante des rapports juridiques privés" (Rigaux, 1988,489). **Cette extension du rôle de l'Etat justifie la consécration explicite ou implicite dans les législations d'Europe occidentale du principe de pertinence applicable aux fichiers du secteur privé et parallèle à ceux déjà décrits en ce qui concerne les fichiers du sectur public .**

28. 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 et néerlandaises.

A la base de la nécessaire consécration de ce principe, repose la constatation suviante : "il ne faut pas perdre de vue que c'est toujours dans un but bien déterminé que les données sont rassemblées, mise 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 pluaprt des législations européennes.

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

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 sécurité exige :

- la consécration de règles déontologiques applicables à toutes les personnes qui ont à approcher les banques de données;
- pour le centres de traitement localisables, la nomination de "gestionnaires", c'est-à-dire des personnes chargées au sein des entreprises et administrations du respect de la réglementation de l'information 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.

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". 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.

B. Evolution des principes

30. Le fondement même de la réglementation des traitements informatiques traitant des données nominatives justifie que le principe de finalité ou de pertinence puisse être apprécié différemment, étant donné les risques nouveaux attachés à des développements récents de la technologie. Pour faire bref, deux exemples nous suffiront : les systèmes experts et les traitements opérés dans le cadre d'opérations télématiques dites "grand public".

a. Principe de finalité et systèmes experts

31. Le développement des sytèmes d'intelligence artificielle ou des systèmes experts suggère quelques réflexions relatives au principe de finalité. Ces systèmes figent dans une procédure automatisée un raisonnement humain : ainsi, un système expert permettra d'évaluer la solvabilité d'un demandeur de crédit ou de déduire certaines informations complémentaires à partir de données minimales relatives à un consommateur ou un groupe de consommateurs.

Il est traditionnel de rappeler à propos de tels systèmes la règle énoncée par l'article 2 de la loi française suivant laquelle "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". Deux réflexions nous apparaissent devoir compléter cette référence légale. Premièrement, l'utilisation de systèmes experts pour identifier non point simplement des individus mais bien des groupes d'individus justifierait l'extension du prescrit aux traitements relatifs à des groupes d'individus. Secondement, il serait utile que l'intéressé soit averti de l'existence d'un système expert et de son utilisation comme outil d'aide à la décision et qu'un contrôle de la qualité de ce système puisse être effectué a priori (système de licence) ou ordonné par un tribunal.

b. Principe de finalité et services télématiques grand public

32. L'analyse de prescrits règlementaires (en projet (ainsi, l'EFT Privacy Act Américain) ou déjà adoptés) relatifs à des **services télématiques** conduit à d'autres réflexions toujours relatives à l'application du principe de finalité. La première, la plus importante, met en évidence la définition a priori par la règlementation des types de traitement permis à ceux qui offrent de tels services. Ainsi, l'article 9 du Bildschirmtextvertrag allemand, applicable aux services videotex grand-public, prescrit que le serveur ne peut traiter les données que pour des besoins de sa facturation et de connaissance statistique de la clientèle. Il interdit la cession des données à des tiers et la constitution d'un profil type client, sauf accord de ce dernier. Il limite la durée de conservation des données.

Cette tendance à définir a priori le contenu des données pertinentes, la durée de leur conservation et les types d'utilisation légitimes peut heurter certains, favorables à la définition libre par entreprise, maître du fichier, des finalités des traitements opérés, et à réserver à un contrôle a posteriori laissé au juge ou à un organisme chargé de contrôler le respect de la légitimité des finalités du traitement. Ce principe d'un contrôle a posteriori a été adopté dans bien des législations, en particulier allemande, autrichienne, danoise, norvégienne, etc...La remise en cause du principe en matière de services interactifs grand public nous semble procéder des craintes renforcées provoquées à la fois par la nature des données enregistrées et leur mode de collecte.

33. La deuxième réflexion s'attache à l'interdiction de proposer certains services télématiques ainsi, l'exclusion du service de sondage à domicile. Dans le même esprit, devraient être interdits certains traitements, ainsi le traitement des données crèées par l'utilisation à distance de jeux video, dans la mesure où leur traitement permettrait la connaissance de la psychologie de l'utilisateur.

34. La troisième est la distinction opérée entre, d'une part, les **partenaires** au service, celui qui offre le service et celui qui reçoit le droit de l'utiliser et, d'autre part, les intervenants à la réalisation du service, ce qu'en matière de T.E.F., le projet américain (l'E.F.T.Privacy Act) qualifie de "EFT Service Provider", c'est-à-dire en l'occurence les commerçants chez qui des terminaux sont installés, les centres serveurs communs à différents prestataires de services, les transporteurs,etc...

La règlementation des traitements opérés par cette seconde catégorie d'acteurs est plus sévère. Leur droit au stockage des données dans le cadre de leur mission est strictement limité et leur sont interdits non seulement la commercialisation des données mais également la constitution de pool de renseignements qui pourraient être utiles aux membres du réseau. Se retrouve ici la distinction opérée dans certaines législations (par exemple, les législations allemande, autrichienne, danoise) entre les entreprises traitant des données pour le compte d'autrui, soumises à une règlementation plus rigoureuse (régime d'autorisation).

IV. Le fondement explicatif reconnu à la protection des données nécessite la reconnaissance d'un lieu de négociation et d'arbitrage : le rôle des autorités de protection des données .

35. Burkert (1984) définissait comme suit l'approche réglementaire souhaitable de la technologie informationnelle (Information Law ou Law of Information Technology), parlant de " **learning systems**", c'est à dire d'une solution législative qui, dans le cadre d'un système réglementaire, établit "an institution provided with competence to collect the information in the regulated area, to make ad-hoc decisions according to rather more generally formulated criteria in a law and to feed back the information collected during the execution of its tasks to society and its rule making agencies. " Ainsi,le système est capable d'apprendre et de s'adapter, concluait l'auteur. Il est clair que le rôle attribué par nos législations d'Europe occidentale aux **autorités de protection des données** correspond à ce souhait. Ces autorités ont de multiples rôles : "chien de garde pour

assurer la légitimité des actions de ceux qui collectent, traitent et distribuent l'information (rôle exécuté soit par la voie d'autorisations générales ou spécifiques et/ou à travers un pouvoir d'investigation); organe consultatif pour le secteur public et parfois également pour le secteur privé), un de ses buts étant de promouvoir des pratiques convenues ensemble en mettant en place des règles relatives à la circulation de l'information; une institution de réglement ou de solution de litiges; un organe avec des pouvoirs indépendants pour créer des normes et disposant d'une compétence pour adapter les principes affirmés par la loi " (Rodota, 1984).

36. Il est évident que cette conception des législations de protection des données et le rôle central attribué à l'autorité de protection des données cadrent parfaitement avec l'analyse proposée : la réglementation de protection des données ne se résume-t-elle pas dans un débat,celui que nous évoquions, entre libertés,la liberté du ficheur et celle mise en péril par la liberté du ficheur, la liberté du fiché . Ce débat ne peut être solutionné une fois pour toutes. Sa solution exige que l'autorité chargée d'arbitrer ce débat puisse peser les intérêts en jeu et ce, au regard d'une évolution technologique qui interdit de figer les solutions mais oblige à apprécier combien celle-ci modifie les équilibres fragiles à peine définis (cf à cet égard, l'évolution préalablement notée,promue par les autorités de protection des données, du droit d'accès et celle du principe de finalité).

37. Ainsi,le rôle essentiel des autorités de protection des données est d'être un **lieu de dialogue et de négociation** . En France, le système des normes simplifiées discutées avec les représentants d'un secteur apparaît comme un mode souple et non contraignant de promouvoir des règles de conduite adaptées aux spécificités d'un secteur . La solution de la récente législation hollandaise et la pratique du Data Protection Act s'inspirent du même principe lorsqu'elles permettent au secteur d'élaborer des codes de conduite dont la ratification est par la suite négociée avec la commission de protection des données . Si ce nouveau rôle des autorités de protection des données nous apparaît indispensable et à élargir, le fait de ne retrouver à la table des négociations qu'une des parties à savoir les ficheurs et la peur de voir ceux-ci s'organiser précisément à l'occasion de cette négociation afin de défendre une position commune font craindre que l'arbitrage ne soit faussé au profit de ces derniers . A cet égard, la transparence des débats et la représentation des fichés sont des exigences incontournables pour que l'autorité de oprotection des donnéespuisse être une pièce maîtresse du dialogue entre ficheur et fiché et aider les uns et les autres à définir une société informationelle plus conviviale .

BIBLIOGRAPHIE SOMMAIRE

- J. BING, International Services Bureaux and T.D.F., Complex 1/85, Norvegian University Press, Oslo.

- J. BING, Impact of Developing Information Technology on Data Protection Legislation. Report prepared for ICCP, OCDE, 1986.

- H. BURKERT, The Law of Information Technology - Basic concepts, Colloque de l'ABDI, Computer and Telecommunications. Is there a lawyer in this Room. 7-10 déc.1987, Travaux et Précis de la Faculté de droit de Namur, Ed. Story Scientia, Bruxelles, n°8, 1989.

- H. BURKERT, Information Law and Information Ethics, La télématique, Actes du colloque de Namur. Travaux et précis de la Faculté de droit de Namur, Ed. Story Scientia, Bruxelles, 1983, T.C.

- H. BURKERT, Datenschutz und informations - und Kommunikationstechnik: Eine Problemskizze. GM.D., Bonn, 1985.

- H. BURKERT, Institution of Data Protection - An Attempt at a functional explanation of European National Data Protection Laws, Computer Law Journal, 1982, vol.3, n°1, 169 et s.

- J.L. BROWN, Implications of the informal nature of payments, Compyter Law Journal, 1980, 2, 153 et s.

- P. CATALA, Ebauche d'une théorie juridique de l'information, Rev.dr.prospectif, 1983, n° 1.

- CNIL, 10 ans d'informatique et libertés, Economica, Paris, 1988, 96.

- D.H. FLAHERTY, Protecting Privacy in Two ways Eletronic Services, Mansell, London, 1985.

- D. FROYSTAD, Data protection in practice : identifying and matching elements, Teresa (17) , Complex N.R.C.C.L., Oslo, 1984 Complex 8/84, Norwegian Univ. Press, Oslo, 1984.

- H. GODSCHALK, Datenschutz am point of sale, Computer und Recht, 1987, n° 7, 416 et s.

- I.B.I., De l'informatique juridique au droit de l'informatique, Document, DR 09, Janv. 1983.

- D.A. MARCHAND, Privacy, Confidentiality and Computers : National and International Implications of U.S. Information Policy, Telecommunications Policy, Sept. 1979.

- Office of Technology Assessment (O.T.A.) Selected Electronic Fund Transfer Issues, Privacy, Security and Equity, Background Paper, Congressional Board, 94th, Congress, 1982

- Office of Technology Assessment (O.T.A.) Electronic Surveillance and Civil Liberties, Congress of U.S., Washington, 1985.

- Y. POULLET, TEF et protection des données à caractère personnel, Rapport présenté au 6ème séminaire de droit à la consommation, EFT and Consumer Protection, L.L.N. 1987.

- Y. POULLET, Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information, Conseil de l'Europe, Conf. d'Athènes, nov. 1987, publiée D.I.T., 1988.

- Y. POULLET, F. WARRANT, Nouveaux compléments au service téléphonique et protection des données: A la recherche d'un cadre conceptuel. Rapport eu Conseil de l'Europe. Jav. 1989.

- F. RIGAUX, La protection de la personne et de la vie privée, Précis, UCL, Faculté de droit, 3 tomes, 1988.

- S. RODOTA, Protection de la vie privée et contrôle de l'information: deux sujets d'inquiétude croissante pour l'opinion publique, Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, OCDE, Etudes d'informatique, n° 10, Paris, 1976.

- S. RODOTA, The Social Challenge of Information Technology, 1984 and beyond, Colloque de l'O.C.D.E., Berlin, Nov. 28-30, 1984.

- S. RODOTA, Protezione dei dati e circulazione delle informazioni, Riv. Crit. del Diritto Priv., 1984, n° 4, 721 et s.

- J.SCHNEIDER, Datenschutz und New Medien, NJW 1984, 390 et s.

- A. WESTIN, Privacy Issues and the implications of Home Banking, American Banker, June 3, 1981.