Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information

Poullet, Yves

Published in:
conférence sur les problèmes législatifs de la protection des données, Athènes, 18-20 novembre 1987

Publication date:
1987

Document Version
le PDF de l'éditeur

LES CONCEPTS FONDAMENTAUX DE LA PROTECTION DES DONNEES ET LES NOUVELLES TECHNOLOGIES DE L'INFORMATION.

Y. POULLET

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

Conseil de l'Europe.
Conférence sur les Problèmes législatifs de la protection des données

Athènes, 18-20 Novembre 1987.

corrigé le 01/10/87

INTRODUCTION

1. Cinq caractéristiques me paraissent définir le développement des technologies de l'information : la **banalisation**, **l'interactivité des services**, la **non transparence**, **l'internationalisation des flux** et **l'accroissement des capacités**.

2. Ainsi, l'informatique n'est plus le seul fait des entreprises et des organisations. Sa convivialité ne la réserve plus aux seuls experts ni ne l'enferme plus dans des locaux à accès réservé. Les outils de traitement de texte et les micro ordinateurs mettent l'informatique à disposition des secrétariats et des ménages. Cette constatation induit trois réflexions sur nos actuelles législations Privacy et en particulier sur les principes mis en exergue par la convention du Conseil de l'Europe.

- Ces réglementations ne sont-elles pas fondées sur la possibilité de localiser facilement a priori les lieux de traitement et de stockage ?

- Ces réglementations peuvent-elles étendre leur champ d'application aux utilisations purement privées et familiales ?

- La lourdeur de certaines de ces réglementations est-elle compatible avec la "trivialisation" des traitements en cause ?

3. La conjonction des capacités de traitement toujours plus grandes de l'informatique et des possibilités de transmission offerte par les réseaux de télécommunication ont permis l'éclosion des services de téléinformatique tant dans le domaine professionnel (accès à des bases de données, télétraitement, courrier électronique) que dans le domaine grand public (transferts électroniques de fonds, services viodeotex).

L'utilisation de ces services justifie deux réflexions

- Les données nominatives en cause sont celles créées par l'utilisation du service lui même : le caractère confidentiel des données ne naît pas,

comme c'était le cas dans le contexte de la quasi totalité des législations "Privacy", du contenu a priori de la banque de données (la plupart des informations contenues au départ sont banales) mais s'attache aux données résultant de l'usage fait par les consommateurs du service (par exemple, un service de télédistribution) et qui viendront l'enrichir, permettant une connaissance du profil type de chaque utilisateur voire de groupes d'utilisateurs, permettant ce qu'un rapport de l'O.T.A. appelle une "Electronic Surveillance".

- L'utilisation de ces services pour la réalisation d'opérations courantes modifie profondément la nature de ces opérations. Nous voudrions le montrer à propos du paiement électronique mais les mêmes réflexions peuvent être adressées à l'opération banale de suivre une émission de télévision lorsque les informations relatives au choix de l'émission,au temps d'écoute,etc.sont enregistrées par la centrale d'un télédistributeur.

La valeur informationnelle d'un paiement au comptant est quasi nulle. Un paiement en espèces ne donne au vendeur aucune indication sur l'identité de l'acheteur et le vendeur peut difficilement établir une quelconque corrélation entre tel individu et tel dépense. Quant au banquier, il reste extérieur à l'acte de consommation sauf dans le cas exeptionnel où l'acquisition d'un bien est lié à l'octroi par lui d'un crédit.

Le paiement par chèque modifie quelque peu la valeur informationnelle du paiement. Le vendeur connait non seulement l'identité de son client mais également la relation qui unit ce client et un organisme financier, en l'occurence l'organisme à l'origine de la délivrance des chèques. De son côté , le banquier dans la mesure où le chèque porte le nom du commerçant a une information sur l'existence d'une relation commerciale entre le client et le commerçant. Cette information reste limitée et sa durée de conservation également.

Dans le cas de transfert électronique de fonds, le paiement acquiert une valeur informationnelle sans commune mesure avec celle relevée pour les autres moyens de paiement. Ainsi, le retrait à un G.A.B. permet au banquier de conserver une trace non seulement de l'identité du retirant mais également du lieu du retrait et de l'heure précise où celui-ci a été effectué. L'utilisation d'un T.P.V. renseigne le banquier sur l'identité du commerçant, l'importance et le moment de la transaction voire sa nature.

A l'inverse, le commrçant peut avoir une information immédiate sur la liquidité du client et sur l'existence d'un compte auprès d'un organisme bancaire. L'utilisation de la technique informatique pour la gestion de telles informations accroit encore leur valeur informationnelle puisque les aggrégations de ces informations primaires, leurs recoupements et leurs comparaisons permettront à leurs détenteurs de se faire une image précise des habitudes de consommation d'un client, de ses déplacements, de l'importance relative de chaque type de dépenses, etc...

4. La non transparence des circuits d'information s'entend en deux sens

- dans un premier sens, elle résulte du fait de la téléinformatique et se traduit par l'existence d'une pluralité des lieux de traitement et de stockage souvent inconnus des utilisateurs des services téléinformatiques;

- dans un second sens, elle constate la **diversification** de plus en plus grande des activités des entreprises, induites par les changements technologiques : les banques ont lancé un peu partout des activités d'agences de renseignements et de voyages, les entreprises, producteurs d'outils informatiques gèrent des réseaux de courrier électronique, sont serveurs de bases de données, etc ... Il est parfois difficile de raisonner encore en termes de secteurs d'activité et de définir une finalité unique aux traitements opérés dans le cadre d'une entreprise.

- dans un troisième sens, elle s'inquiète des développements des cartes à microprocesseur déjà employées en matière médicale mais également pour d'autres fonctions (cartes de crédit, cartes administratives "étudiant"). Ces véritables cartes d'identité peuvent masquer à leur porteur leur contenu exact et le problème de la modification et de l'accès à leur contenu se trouve posé.

5. La circulation de l'information permise par les télécommunications ajoute à la non transparence des lieux de stockage et traitement, la nécessité de prendre en considération la dimension internationale des flux d'informations. Les services informatiques peuvent être désormais offerts sans considération de frontières et le traitement de l'information peut être opéré tantôt dans tel pays, tantôt dans tel autre pays.

Si, d'une part, les réglementations "Privacy" ne peuvent être un obstacle à ces opérations transfrontières reconnues nécessaires, d'autre part, il est important que des protections équivalentes soient accordées dans les différents pays, afin que ne puissent se créer des paradis de données.

6. Enfin, l'augmentation des capacités de traitement et de stockage autorise des recherches de nature différente, non basées sur un identifiant personnel mais sur des caractéristiques définies a priori pour un "groupe de personnes". On connaît le cas allemand du "Rasterfahndung" (matrix search) utilisé pour la localisation d'un terroriste allemand, Rudolf Clement WAGNER où le recoupement de données de consommation électrique permit à la police la découverte du terroriste. L'utilisation de cette même méthode par des entreprises leur permettra de mieux cibler leur clientèle, de définir les personnes à prospecter pour tel produit, etc ...

7. C'est sur fond de telles considérations qu'est entreprise une analyse du texte de la Convention. En définitive, les concepts fondamentaux de la protection des données tels que définis dans la Convention permettent-ils de donner une réponse appropriée aux craintes suscitées par le développement des nouvelles technologies de l'information ?

La structure de la convention justifie le plan de notre exposé:

- définitions et champ d'application de la convention (article 2 de la Convention) ;
- principes quant à la mise sur pied et la réalisation des opérations (article 5 à 7 de la Convention);
- principes quant au droit d'accès de la personne fichée (article 8 de la Convention);
- principes quant aux flux internationaux relatives à ces opérations (article 12 de la Convention).

I. DEFINITIONS ET CHAMP D'APPLICATION

8. Trois notions sont examinées,celles de **données à caractère personnel,de fichier automatisé** et celle **de maître du traitement.**

La notion de "données à caractère personnel"est définie comme l'"information concernant la personne physique identifiée ou identifiable".Une telle définition permet de comprendre dans le champ d'application de la Convention tout moyen technique d'identification d'une personne physique,ainsi outre le nom,la reconnaissance de la voix,la reconnaisance dynamique de la signature,les empreintes digitales ou tout autre procédé d'identification,ce que le Privacy Act américain qualifie de **"record"**.

De même,lorsque le moyen d'identification est utilisable par un groupe notamment familial(par exemple,dans le cas de terminaux videotex installés à domicile),dans la mesure où l'attitude de chaque membre du groupe est identifiée à celle du groupe,la notion s'applique à de telles données.

Enfin,pour faire écho aux cas cités précédemment où comme dans l'hypothèse du "Rasterfahndung",le traitement a pour but principal l'identification d'un groupe de personnes ayant des caractéristiques communes ,il nous semble que la définition reste valable puisque le traitement concerne des personnes identifiables non peut être en tant que telles mais en tant que membres d'un groupe. Nous aurons l'occasion de revenir sur ces hypothèses qui exigent d'autres réflexions relatives à certains principes de la convention(Cf. infra, n°)

9. Le **fichier automatisé** s'entend de "tout ensemble d'informations faisant l'objet d'un traitement automatisé".Cette définition prend comme critère la procédure de traitement de l'information et à la limite comprend toute forme d'enregistrement des données permettant certaines opérations sur ces données,ainsi un traitement de texte serait un fichier automatisé .Sans doute serait-il utile d'inclure dans la définition un critère supplémentaire afin de ne pas soumettre à réglementation certaines applications informatisées courantes mais ne présentant manifestement

pas de dangers pour les individus.

A cet égard,faut-il s'en tenir au critère de l'organisation a priori des données personnelles et exclure toute application non structurée en base de données ? Une telle conclusion serait dangereuse. Les méthodes de traitement modernes permettent d'appliquer même à des textes non structurés des méthodes de recherche automatisée.Ainsi,à un programme de traitement de texte peut être couplé un programme permettant d'extraire certaines données et de les corréler.En d'autres termes,c'est le critère de la **"retrievability"** attaché non à un programme mais à un ensemble cohérent de programme qui doit être adopté à l'instar de la loi norvégienne par exemple.

10. Une toute autre question est soulevée à propos de cette notion de fichier automatisé.Les récents travaux du Conseil de l'Europe sur l'impact de la télémétrie,des médias interactifs et des systèmes de courrier électronique y font allusion et leurs réflexions peuvent être étendus à tout service télématique.La notion de fichier automatisé suggère l'existence d'un fichier centralisé ,facilement localisable.Or,par exemple en matière de T.E.F.,les lieux de traitement de l'information née de l'utilisation du service ou nécessaire à sa réalisation sont multiples :fichiers locaux sur les T.P.V.,centre de stockage ou de tri à la fois sur les réseaux publics et privés(ceux des mandataires techniques),centre informatique bancaire régional,etc..

Dans la mesure où tous ces lieux dialoguent dans le cadre d'un système informatique réparti et que l'ensemble des ces traitements concourent à la réalisation d'une même opération,il est important que la notion de fichier ne soit plus liée à celle de lieu de traitement mais bien à celle d'ensemble fonctionnel d'un ou de plusieurs traitements.Les travaux suggèrent la notion de **"fichier logique"**,"permettant de situer en dernier ressort,à travers des méthodes d'extraction,toutes les données dispersées dans le réseau suite à un traitement et à un enregistrement légitimes au sein d'une organisation donnée".

11. Dans le même sens,et afin de rendre plus claire l'influence du réseau sur le traitement des données nécessaires ou créées lors de l'utilisation du service électronique de paiement,il est important de redéfinir, en ce qui

concerne particulièrement les services télématiques,la notion de **maître du fichier** comme **maître du réseau**,responsable de l'ensemble des données à caractère personnel reprises dans le réseau,c'est à dire de ce que nous venons d'appeler le fichier logique.

L'idée d'un responsable unique vis à vis des fichés , de l'ensemble des traitements créés par la mise sur pied et la réalisation de service électronique et de leur conformité à la réglementation de protection de données rejoint celle développée par la doctrine à propos des questions de responsabilité civile en cas d'erreur ou de fraude dans l'exécution du service . Elle s'inspire du même souci de faciliter l'information,l'accès et les recours de l'utilisateur de ces services et désigne tout naturellement l'organisme qui octroie l'accès au service comme responsable pour l'ensemble du réseau.

La notion de maître du fichier peut-elle s'appliquer à une personne physique qui, dans le cadre d'une **utilisation à titre purement privé**, tient sur un micro computer son agenda,la liste de ses amis et autres traitements personnels ? La banalisation déjà signalée de l'utilisation de l'informatique invite à poser la question. Les limites que posent la Convention à la liberté de traiter les données ne peuvent s'appliquer aux traitements purement privés puisqu'elles représenteraient une atteinte à la liberté individuelle. Ceci n'exclut pas que certains traitements faits à domicile dans le cadre d'activités professionnelles (par exemple,dans le cas de télétravailleurs) soient soumis à réglementation.

Enfin,la notion de maître du réseau comme personne "compétente pour décider quelle sera la finalité du fichier automatisé,quelles catégories de données doivent être enregistrées et quelles opérations leur seront appliquées" s'applique difficilement dans le cadre de **services de courrier électronique**,puisque le contenu et la destination des messages sont le fait des participants au service. Il est utile de s'interroger sur la nécessité d'appliquer à ces services les réglementations privacy. En effet,ces services sont des services de correspondance privée et ,dès lors, le courrier électronique doit bénéficier des mêmes garanties de confidentialité que celles offertes par les lois voire les constitutions nationales . Ces garanties impliquent que tout transporteur qu'il soit public ou privé prenne des mesures de sécurité contre l'interception des messages par un tiers et interdise le déchiffrement des messages à toute personne non autorisée.

II. PRINCIPES LORS DE LA MISE SUR PIED ET DE L'UTILISATION DES TRAITEMENTS

12. Nous retiendrons trois principes:
-le principe de la **collecte par des moyens licites et loyaux**(article 5a));
-le principe de **finalité** dans l'enregistrement et la durée des traitements(article 5b),c)et d));
-le principe de **sécurité des données**(article 7).

A. Le principe de la collecte par des moyens licites et loyaux.

13. L'introduction insistait sur le fait qu'en matière de services télématiques en particulier,les données les plus sensibles étaient créées par l'utilisation des services. Cette constatation souligne l'importance de rendre l'utilisateur conscient des données nominatives qui seront recueillies lors de l'utilisation de tels services et de la finalité de leurs traitements.Ainsi se dégage la double idée premièrement d'une **transparence des circuits d'informations** et de la nature de celles-ci et secondement d'un **consentement libre et éclairé** du fiché dûment informé de l'existence de tels traitements. Cette double idée légitime les réglementations adoptées dans certains pays vis à vis de certains services télématiques(Cf. par exemple la loi danoise sur les cartes de paiement,le Cable Communication Policy Act américain)et obligeant les entreprises offrant de tels services à donner des informations étendues sur les données recueillies,le réseau et les traitements y pratiqués.

Ce principe prend une signification particulière en matière de cartes à mémoire.Il ne peut être admis que soient introduites dans la carte des informations secrètes et codées inconnues du détenteur.Ce dernier doit connaître les types d'information admises à figurer sur la carte et les personnes habilitées à les lire. Ainsi, la lecture de certaines zones

d'informations figurant sur une carte de paiement peuvent être réservées à la lecture par les commerçants à l'exclusion des banquiers et vice versa.Le même principe vaut a fortiori pour les cartes médicales et d'autres applications de la carte à mémoire .

B. Le principe de finalité.

a. ...et les systèmes experts.

14. Le développement des systèmes 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. 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) ... et les services télématiques grand public .

15. L'analyse de prescrits réglementaires (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 réglementation 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 du 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 l'entreprise, maître du fichier, des finalités des traitements opérés, sous contrôle a posteriori par le juge ou par un organisme chargé du contrôle. Ce principe d'un contrôle a posteriori a été adopté dans bien des législations, en particuliers 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.

16. 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 créées par l'utilisation à distance de jeux video, dans la mesure où leur traitement permettrait la connaissance de la psychologie de l'utilisateur.

17. 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'EFT 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 réglementation des traitements opérés par cette seconde catégorie d'acteurs est plus sévère. Leur droit du stockage des données dans le cadre de leur mission est strictement limité et leur est interdit 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 dans le cadre de leurs activités propres et celles traitant des données pour le compte d'autrui, soumises à une réglementation plus rigoureuse (régime d'autorisation).

c) ... et la tendance aux accords de coopération.

18. Cette distinction apparaît d'autant plus nécessaire que se multiplient les **accords de coopération** entre entreprises offrant des services télématiques. La remarque déborde le cadre des seuls services télématiques grand-public. La nécessité de définir des normes de transmission commune et de proposer, à différentes entreprises d'un secteur voire à toutes, des services de communicaton (service de courrier électronique, base de données partagées, etc...) expliquent le fait que se multiplient la création de services communs à plusieurs entreprises, parfois érigées en sociétés distinctes. Ces accords de coopération s'expliquent également par le coût des investissements nécessaires à la mise sur pied de tels services. Ils portent sur le partage des faits de recherche et de développement.

19. Ainsi, la transmission des données à caractère personnel dans le cadre de ces réseaux ne peut avoir pour but la création de vastes centres de renseignements communs aux participants du réseau.

d) ... et la diversification des activités des entreprises.

20. Pour terminer nos réflexions sur le principe de finalité, nous voudrions mettre en exergue une conséquence de la diversification des activités des entreprises, fruit notamment de leur utilisation des nouvelles technologies. L'exemple des medias est remarquable à cet égard ; la presse écrite a bien souvent pénétré le domaine de l'audiovisuel, offre des services on line, etc... Rares sont les banques qui n'offrent pas des services d'agences de voyages voire de renseignements commerciaux.

Cette despécialisation des activités engendre la crainte que les traitements opérés dans le cadre d'une activité ne soient également

utilisés dans le cadre d'une autre activité et servent à compléter les informations sur les individus. Il est important que de la même manière certaines législations exigent de certaines entreprises (par exemple la législation canadienne relative aux entreprises de télécommunication) des comptabilités séparées pour éviter toute subsidiation croisée, les autorités chargées du contrôle des données imposent au nom du principe de finalité que des distinctions claires soient opérées entre traitements et que des maîtres de fichiers différents soient responsables des traitements propres à chaque activité de l'entreprise.

C. Le principe de sécurité.

21. La particularité des traitements opérés dans le cadre d'un service télématique met en évidence la dissémination des lieux de traitements et pour certains lieux la totale impossibilité de prévoir des systèmes de sécurité physique (par exemple: G.A.B. situés dans les lieux publics).

L'obligation imposée de prévoir des "moyens de sécurité" adéquats oblige à envisager l'ensemble du ou des réseau(x) de transmission de l'information, y compris la carte d'accès. En particulier, s'il s'agit d'une carte à mémoire, le fournisseur du service s'engage à prendre toutes les précautions pour que seules les personnes autorisées puissent avoir accès aux informations reprises dans la mémoire (C.N.I.L., 5° rapport d'activités, 1985, p. 150). En ce qui concerne la transmission des informations, l'adoption de certaines clés de sécurité (méthodes de chiffrement) pourrait être rendue obligatoire pour certaines opérations.

Vu que, dans ce domaine, un intérêt public important est en jeu, la contrainte juridique devrait émaner d'une réglementation directe ou indirecte (agrément, licence). Cette dernière solution plus souple et plus respectueuse de l'évolution de la technique, s'inscrirait dans le cadre d'un recommandation faite à la Communauté Européenn (cf. rapport MONVILLE-POULLET préparé dans le cadre de FAST: LA DEMANDE FINALE EN TELEMATIQUE) d'une labellisation des centres serveurs (les mandataires techniques en particulier) sur base d'un plan de sécurité défini par ces instances normalisatrices au travail desquelles devraient être associées les autorités chargées de la protection des données.

III . LE DROIT D'ACCES.

_22. Par droit d'accès,on entend au sens le plus large toute mesure visant, d'une part ,à assurer une transparence adéquate pour le fiché des informations et des traitements opérés par le maître du fichier de même que les procédures facilitant les recours en cas d'informations incomplètes,fausses ou non pertinentes.

L'examen du principe de collecte par des moyens licites et loyaux a déjà permis, en matière de services interactifs,de dégager un certain nombre de recommandations visant à la transparence non seulement des informations collectées mais également des circuits que l'information emprunte pour la réalisation de l'opération. La notion de maître du réseau permet de désigner un seul interlocuteur auprès duquel s'exercera le droit d'accès et chargé de rectifier dans l'ensemble du réseau l'information en question.Enfin,tant la diversification des activités des entreprises que la multiplication des accords de coopération entre entreprises offrant des services télématiques oblige à accorder une attention particulière à l'exercice effectif du **"droit de suite"**.

23. La mise en place de services interactifs grand publics de plus en plus nombreux suggère une nouvelle **modalité de mise en oeuvre du droit d'accès**.Ne pourrait-on contraindre les serveurs à mettre à disposition sur un page écran appelable gratuitement toutes les informations relatives aux traitements et habituellement communiquées par écrit (nature des données traitées,nom du responsable,but des traitements) voire permettre à l'utilisateur d'excercer directement par terminal interposé son droit d'accès.

23 bis. 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 "Santés". 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 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.

23 ter. Ainsi, la création de nouveaux modes de collecte, de dissémination et de consertation 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.

Le droit d'accès peut s'élargir au droit au consentement. A cet égard, on rapprochera l'exemple de la carte à mémoire "santé" d'un autre débat : celui des nouveaux compléments au service téléphonique permis dans le cadre RNIS. Les autorités de contrôle de protection des données ont affirmé là également : le principe du consentement des abonnés au téléphone à voir apparaître leur numéro d'appel lors d'une communication téléphonique.

Le débat autour des nouveaux services téléphoniques ou télématiques a mis en relief une autre facette du droit d'accès : celui du "droit à l'anonymat". L'utilisateur d'un service public de télécommunication doit pouvoir bénéficier de méthodes d'utilisation anonymes, ainsi le service 3615 du Minitel ou les cartes préchargées permettent-t-elles à l'utilisateur de ne pas être reconnu de l'offreur de services.

IV . ASPECTS INTERNATIONAUX

_24. Certes,dix pour cent seulement des flux transfrontières concernent des données à caractère personnel. L'augmentation de tels flux est cependant évidente;d'une part,certains services interactifs sont offerts internationalement et d'autre part,les télécommunications accroissent dans une mesure considérable les connexions entre ordinateurs situés dans différents pays.

Une telle constatation explique la volonté d'instances internationales comme le Conseil de l'Europe non seulement de définir des standards communs de protection des données permettant entre pays ayant adopté des normes équivalentes de rejeter toute restriction aux flux transfrontières,fondée sur la protection des données,mais également -et cette seconde tâche reste à accomplir- de promouvoir des **règles de droit international privé**,fixant de façon uniforme les critères relatifs au choix du droit applicable et ,surtout, le **domaine d'application** des législations nationales .

25. La lecture de l'article 12 de la Convention du Conseil de l'Europe suggère une réflexion supplémentaire. Il prévoit que pour certaines données ou certains types de traitement,des dérogations à la liberté des flux transfrontières peuvent être admises pour autant que la législation du pays en cause ne prévoit pas une **protection équivalente**. En matière de services interactifs grand public,se sont multipliées de telles dérogations.Ainsi,en matière de T.E.F., le Payment Act danois obligeles banques qui offrent de tels services à localiser leurs traitements dans le pays sauf exception admise par le Ministre de l'Industrie;en matière de services Videotex,le projet de loi autrichien soumet d'office les serveurs étrangers à suivre les dispositions de la loi autrichienne sur la protection des données .

Cette tendance oblige à mieux définir ce que l'on entend par protection équivalente :s'agit-il d'une protection identique ou au contraire simplement similaire?En toute hypothèse,est soulignée l'importance en ces matières où l'offre de services revêt nécessairement une dimension internationale, de définir des normes communes de façon à éviter tout

"réflexe "réglementaire nationaliste. L'adoption d'instruments souples tels que des **règles de conduite**(codes of practice) définis par le secteur lui même (par exemple le Code of Practice proposé par Eusidic en matière de courrier électronique) est à encourager.

BIBLIOGRAPHIE SOMMAIRE

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

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

-H. GODSCHALK, Datenschutz am point of sale, Computer und Recht 987, n° 7, 416 et s.

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

-Y. POULLET, Privacy et services électroniques d'information, in Electronic information Services: Legal Aspects, Report prepared for the Legal Observatory of the European Commission, Janv. 1987.

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

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

-O. 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.

-S. RODOTA Protezione dei dati e circulazione delle informazioni , Riv.

Crit. del Diritto Priv., 1984, n° 4, 721 et s.

-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, Datenschutz und Informations- und Kommunikationstechnik: Eine Problemskizze. G.M.D., Bonn, 1985.

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

-Office of Technology Assesment, Electronic Surveillance and Liberties, Congress of U.S., Washington, 1985.