T.E.F. et protection des données à caractère personnel

Poullet, Yves

Published in:
Transfert électronique de fonds et protection du consommateur

Publication date:
1987

Document Version
le PDF de l'éditeur

1. TEF ET PROTECTION DES DONNEES À CARACTERE PERSONNEL

Yves POULLET[1]

CDC 22 TEF et protection des consommateurs
6ème Semin. Cycle sur le droit de la consommation. 1987
Story Scientia, Bruxelles, 1988

[1] Directeur, Centre de Recherches Informatique et Droit, Namur, Belgique.

INTRODUCTION
LA VALEUR INFORMATIONNELLE DU PAIEMENT ÉLECTRONIQUE

Au point de départ de notre réflexion sur les questions que posent les transferts électroniques de fonds vis-à-vis de nos libertés individuelles, se pose la constatation que l'utilisation par les individus de ces nouveaux moyens de paiement ont radicalement modifié la nature même de l'acte de paiement (BROWN, GOLDSHALK).

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 telle dépense. Quant au banquier, il reste extérieur à l'acte de consommation sauf dans le cas exceptionnel où l'acquisition d'un bien est liée à l'octroi par lui d'un crédit.

Le paiement par chèque modifie quelque peu la valeur informationnelle du paiement, le vendeur connaît non seulement l'identité de son client mais également la relation qui unit ce client et un organisme financier, en l'occurrence 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. Le contenu de cette information reste limité et, sauf exception, sa durée de conservation, également.

Dans le cas d'un 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 commerçant 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 conservation et la gestion de telles informations accroît encore leur valeur informationnelle puisque les aggrégats 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...

En d'autres termes, du fait de leur valeur informationnelle directe et indirecte, les services de télébanking soulèvent certains dangers pour la protection des données nominatives ; certains de ces dangers sont communs à l'utilisation de tous les services télématiques parmi lesquels se rangent le service de télébanking mais également l'accès à des bases de données informationnelles ou les multiples services de télétransaction, d'autres sont spécifiques à ce service particulier.

Le premier chapitre met en évidence les dangers nés de l'utilisation ou de la réalisation des opérations de télébanking dites grand public. Le second chapitre analyse les réglementations applicables en la matière et en propose une évaluation.

SECTION 1
LES DANGERS PARTICULIERS AUX OPÉRATIONS DE T.E.F.

L'utilisation de n'importe quel service télématique permet de connaître les moments d'interrogation, les moments de présence à domicile, etc. Le contenu des services de télébanking permet d'inférer des craintes nouvelles, ainsi les habitudes de consommation, le montant des transactions, la composition du patrimoine et la façon de le gérer peuvent dorénavant être connus. La localisation des guichets automatiques et des terminaux points de vente permet de contrôler le déplacement des consommateurs.

Comme le note l'O.T.A. américain : « With increased use of E.F.T. there will be a large number of points at which traditional norms of privacy could be invaded. More E.F.T. Terminals will be on-line, making Electronic Surveillance a more credible possibility. Single Statement reporting of all kinds of financial transactions will become common ; more data will be aggregated and thus easier to access. At the same time, there could be broader and swifter dissemination of inaccurate data, even if customer correction of data is facilited, it will be more difficult for corrections to catch up with and replace faulty information ».

Ces dangers particuliers s'expliquent aisément lorsqu'on considère les types de données propres aux services de télébanking (1) et leurs lieux de traitement ou de stockage mettant en évidence la disparité des acteurs et de leurs intérêts respectifs (2).

Les données traitées et la disparité des acteurs constituent en effet les deux particularités essentielles qui justifient l'attention particulière accordée au problème de la protection des données dans la mise sur pied et la réalisation de services télématiques grand public (BING, POULLET).

Premièrement, les données nominatives sensibles sont celles créées par l'utilisation du service lui-même : le caractère confidentiel des données ne naît pas tant 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 de la banque de données et qui viendront l'enrichir permettant une connaissance du profil type de chaque utilisateur voire de groupes d'utilisateurs.

Secondement, l'utilisation de ces services se caractérise par une non transparence des circuits d'information par lesquels passe l'information née de l'utilisation du service télématique, ceci pour deux raisons principales :

— le producteur commercial du service n'est pas nécessairement le même que celui qui permet la réalisation technique du service : la remarque vaut pour la plupart des services télématiques. Ainsi en matière de services télématiques informationnels, à l'agence de presse qui collecte et structure les informations, s'ajoute l'entreprise informatique ou de télécommunications qui connectera ses ordinateurs et logiciels d'interrogation au réseau et permettra de ce fait l'interrogation ;

— l'information demandée ou créée par l'utilisation du service peut être stockée à divers endroits, emprunter des réseaux internationaux par des chemins souvent non établis une fois pour toutes, les modifications pouvant être dues à des variations tarifaires, à l'encombrement de certaines parties du réseau, etc.

Les points 1 et 2 appliquent ces considérations au cas particulier des services électroniques bancaires.

1. Les types de données

En ce qui concerne les types de données, on distingue celles créées a priori du fait même de l'octroi de la carte ou simplement du n° d'accès qui permet l'utilisation du service et celles créées a posteriori par l'utilisation du service.

Certaines informations nominatives sont en effet réclamées lors de l'octroi du n° d'accès ou du code confidentiel (PIN) généralement nécessaire pour l'utilisation des services de télébanking qui nécessitent pour leur fonctionnement une identification personnelle a priori de l'utilisateur. Elles le sont généralement dans le cadre d'un questionnaire rempli préalablement à la signature du contrat d'adhésion.

Les informations nominatives collectées lors de la demande du code d'accès portent sur la profession, l'âge, le nom et la qualité des personnes autorisées, elles identifient le compte. De façon générale, on peut les qualifier de banales.

A l'inverse, les informations créées par l'utilisation du service sont plus diverses et suscitent plus de craintes. On distingue parmi ces informations, celles créées lors de l'utilisation du service et celles créées postérieurement par l'exécution même du service.

A propos des premières, on distinguera :

— les données de transmission peu dangereuses, il s'agit d'informations ajoutées pour assurer la correcte transmission du message et donc nécessaires à la commutation de celui-ci.

— les données de gestion reprenant le n° de compte, le Personal Identification Number (PIN), etc...

— les données relatives au contenu du message, l'opération effectuée, leur nombre variera suivant la technologie utilisée (simples cartes magnétiques ou cartes à mémoire).

Ces informations concernent principalement l'utilisateur (auteur de la création des données) mais également pour certains services des tiers (ex. : identification du bénéficiaire du paiement en cas de virement électronique et surtout en cas de service P.O.S.).

Quant aux secondes, il s'agit essentiellement de données de facturation (en matière de téléshopping) ou de données agrégées reprenant la consommation mensuelle de carburant ou la ventilation par type de transaction des dépenses d'un client. Si en principe elles ne concernent que les utilisateurs et non les tiers, on peut cependant imaginer et la technique rend possible de tels développements, que des tiers, en particulier certains commerçants, puissent obtenir de telles données soit auprès de leurs banquiers soit directement en ayant accès à une « zone » de la carte à mémoire utilisée pour le paiement.

2. Les lieux de traitement ou de stockage

L'introduction du chapitre mettait en évidence la non transparence des circuits qu'empruntait l'information nominative créée par l'utilisation du service télématique.

a) La pluralité des lieux

La vérité de cette assertion appliquée aux T.E.F. est patente : les données créées par l'utilisation du service sont acheminées et traitées en de multiples endroits et chez de multiples intervenants souvent non connus du public utilisateur. Aux intervenants réduits dans les schémas les plus simples : schéma à deux personnes dans les services de Home-Banking ou les G.A.B. schéma triangulaire dans les T.P.V., s'en ajoutent d'autres et ce principalement pour trois raisons.

La première raison a égard à l'organisation collective et hautement complexe de l'installation et de la gestion de ces nouveaux systèmes de paiement : les relations individuelles entre les clients et leurs banques sont dès lors encadrées par les relations contractuelles ou d'associations des partenaires au système (MOSCHEL, SCHNEIDER). Ainsi les banques dans le cadre de ces systèmes T.E.F. participent généralement à un réseau interbancaire dont la gestion est confiée à un mandataire technique.

Une deuxième raison est institutionnelle, les législations européennes exigeant le transit des mouvements interbancaires par une chambre de compensation.

La troisième est d'ordre technique : le transfert des données se fait via des réseaux de télécommunication dont la propriété n'appartient ni aux banques ni à leurs mandataires techniques mais le plus souvent du moins dans nos pays à des entreprises publiques de télécommunication.

On ajoutera que dans les cas de T.P.V., le traitement et le stockage peuvent être faits en succursales mais également être intégrés dans un centre commun à toutes les succursales ou filiales voire à différentes compagnies.

La présentation de cette pluralité des lieux de traitement et de stockage doit être complété d'une analyse des acteurs concernés par le transit ou intéressés par ces données.

b) Les intérêts des acteurs

Participant à la réalisation de l'opération, cinq acteurs semblent avoir des intérêts distincts parfois complémentaires : d'abord le fournisseur du service (la banque ou l'organisme émetteur de cartes de crédit), son ou ses mandataires techniques et l'utilisateur du service (le possesseur du n° d'accès) ; ensuite, en cas de T.P.V., le commerçant chez qui le terminal d'accès à ce service de télébanking est installé ; enfin, le tiers bénéficiaire occasionnel d'un service de télébanking.

Pour être complet, on notera que certaines administrations, dans le cadre de l'application de la loi fiscale par exemple, et la justice non seulement dans le cas de litiges concernant les opérations à la base de l'utilisation de ces services mais également dans le cadre d'enquêtes pénales peuvent avoir intérêt à accéder aux informations créées à l'occasion de l'utilisation de ces services.

— la banque ou l'organisme émetteur de cartes de crédit

Trois intérêts majeurs plaident en faveur du stockage des informations nominatives par le fournisseur du service.

Tout d'abord, son souci d'avoir une comptabilité analytique la plus complète possible, c'est-à-dire pour chaque opération télématique explique le stockage et la conservation des données de l'opération. Cette comptabilité analytique est nécessaire pour assurer le suivi des opérations (exécution d'ordres de paiement).

Ensuite, la trace conservée de l'opération lui servira de preuve de l'opération impulsée par l'utilisateur tant au regard de l'utilisateur lui-même, qu'au regard des lois comptables existantes dans chaque pays. On notera que les exigences de preuve peuvent varier dans les deux cas. Face à l'utilisateur, il se doit de conserver une trace la plus complète possible. Face à l'administration, la nécessité de conserver ne s'étend peut être pas à un aussi grand nombre d'informations.

Enfin, les informations nominatives nées de l'utilisation des services de téléshopping et de télébanking permettent au fournisseur de services une excellente connaissance de sa clientèle, c'est-à-dire que vis-à-vis de ses clients utilisateurs privés détenteurs de cartes, le traitement de ces informations induit pour la banque la possibilité de connaître leurs habitudes de consommation (type, nature, localisation, voire le détail des opérations pratiqués par eux) ; c'est-à-dire que cette fois vis-à-vis de ses clients professionnels détenteurs de T.P.V., ces informations permettront à la banque de connaître leur part de marché, le type de leur clientèle et, de façon générale par extrapolation, l'évolution de leur chiffre d'affaires.

Ainsi, l'institution financière dispose de renseignements utiles

— pour évaluer la diffusion de ses propres services électroniques financiers et développer leur marketing ;

— pour le marketing d'autres produits auprès de sa clientèle professionnelle et privée dans la mesure où elle la connaît mieux ;

— pour déterminer le crédit de cette clientèle.

— L'utilisateur du service

Outre les avantages indéniables que lui offre le moyen électronique de paiement par rapport aux autres moyens de paiement, l'utilisateur trouve — il faut bien le reconnaître — certains avantages à un bon traitement des informations créées par son utilisation du service.

A l'avantage technique immédiat que procure le traitement des données d'identification pour la sécurité et pour la continuité du service (l'utilisateur, en cas de rupture de la communication, peut reprendre le dialogue où il l'a laissé), le fait pour l'utilisateur de recevoir à intervalles réguliers copie de ces informations stockées chez le fournisseur l'aide à gérer son budget, lui permet de suivre ses dépenses voire d'obtenir la preuve vis-à-vis des commerçants, en cas de contestation du paiement ou de la réalité de la transaction ; cette preuve des opérations effectuées est également utile vis-à-vis de certaines administrations (fiscales en particulier, exemple : dépenses mensuelles de carburant).

Il opposera à ce traitement des données nominatives certaines objections :

— ce traitement peut affecter sa liberté d'obtenir du crédit, par exemple en cas de conservation trop longue de certaines données (ex. dépassements répétés de la provision conservés) mais surtout en cas de pratiques de crédit scoring, excluant automatiquement certains clients sur base de certaines dépenses ou de certaines habitudes de consommation) ou plus simplement sa liberté d'accéder au service électronique en conséquence du ciblage de clientèle ;

— il peut craindre que ce traitement ne garantisse pas l'anonymat de certaines opérations (ainsi, le donateur qui veut que son virement électronique reste anonyme) ;

— ce traitement peut affecter d'autres libertés individuelles, ainsi la liberté d'opinion (l'information : abonnement à tel journal peut renseigner des tiers sur les tendances philosophiques, politiques ou religieuses de l'utilisateur du moyen de paiement) voire la liberté de déplacement (contrôle des déplacements), etc.

— Le commerçant

Outre la garantie de paiement souvent attachée à la carte de crédit, l'installation d'un T.P.V. chez un commerçant s'explique pour diverses raisons. La première est bien évidemment, celle de faciliter la gestion comptable de ce commerçant. A celle-là, s'en ajoutent d'autres (sur ces différents motifs, Priewasser) : le commerçant souhaite connaître sa clientèle (les habitudes de consommation de chaque client) pour des raisons de marketing. Enfin, il souhaite conserver en cas de litige une preuve de l'opération, preuve d'autant plus irréfutable qu'elle est détenue par un tiers.

— Les bénéficiaires

Pour des raisons diverses, le tiers bénéficiaire d'un virement électronique peut craindre que le traitement automatique via un service de télébanking ne permette aux fournisseurs de service d'obtenir des renseignements sur lui-même (contrôle automatique des sources de revenus). La même crainte s'étend vis-à-vis d'autres intervenants, le mandataire technique voire la banque du donneur d'ordre.

— Le mandataire technique

La bonne gestion du réseau implique le stockage par les mandataires d'un certain nombre d'informations ; ainsi, il est clair que le mandataire doit garder la trace des opérations effectuées à partir des terminaux connectés afin d'assurer leur exécution ; également, il doit tenir une information la plus à jour possible non seulement sur l'état des comptes des titulaires de moyens électroniques de paiement afin de prévenir des débits non autorisés mais également, sur les cartes perdues ou volées afin de détecter d'éventuelles fraudes.

Il est évident qu'à partir de ces informations relatives aux clients appartenant bien souvent à différentes institutions financières, le mandataire technique pourrait avoir une vue bien plus complète encore que celle de chaque membre du groupe sur leurs différents clients professionnels et privés et pourrait songer à offrir aux membres du groupe voire à des tiers une information plus fine encore que celle à la disposition de chaque membre.

— L'administration en particulier fiscale

Pour les besoins de l'application de lois fiscales, on peut concevoir que l'administration puisse avoir intérêt à accéder aux traitements des données créées dans le cadre de l'utilisation des services télématiques en question. Il s'agira de vérifier les opérations faites tantôt par les commerçants, tantôt par les utilisateurs.

On notera à cet égard que c'est pour cette raison notamment que la loi de finances de 1984 a ajouté à la liste des moyens de paiement obligatoirement acceptables par le commerçant, la carte de paiement électronique.

— Les juges

La production des traitements informatisés peut poursuivre deux buts : démontrer l'existence d'une opération contestée au civil ou au pénal ou vérifier la présence contestée d'une personne à tel endroit ou à tel moment (cf. par exemple, dans le cas d'une procédure pénale).

Cette présentation de la spécificité de l'opération de T.E.F. attire l'attention sur la difficulté d'une réglementation de la protection des données en la matière. Celle-ci se doit de prendre en considération la particularité des données et la diversité des acteurs. Ensuite, dès maintenant, il apparaît que les intérêts de l'utilisateur, en particulier de sécurité et de protection des consommateurs, peuvent contredire les exigences de la protection de sa vie privée et, dès lors, nécessitent qu'un choix soit fait entre des objectifs parfois contradictoires.

Ainsi, l'utilisateur peut souhaiter, au nom de ses intérêts de consommateur, obtenir un relevé mensuel des différentes opérations effectuées à partir de terminaux mais doit autoriser alors le traitement et le stockage des informations relatives à ces opérations.

Ainsi, des organismes de carte de crédit (cf. les exemples cités par GOLDSCHALK) détectent des vols de cartes par l'enregistrement automatique des déplacements du porteur de la carte et la comparaison avec le profil type de leur client, offrant dès lors à ceux-ci une sécurité supplémentaire.

SECTION 2
RÉGLEMENTATIONS « PRIVACY » ET T.E.F.

Les réflexions du premier chapitre et de l'introduction laissent clairement entendre qu'une réglementation « privacy » appropriée est nécessaire pour les T.E.F., étant donné la spécificité de ces opérations, nonobstant les déclarations du groupe de travail australien chargé d'examiner les problèmes juridiques soulevés par les transferts de fonds.

Dès 1977, la National Commission on E.F.T. américaine résumait comme suit les enjeux occasionnés par le développement des T.E.F. :

« — E.F.T. will create records of financial transactions where there were none before ;

— E.F.T. may increase the amount of information currently included in financial records ;

— E.F.T. records in electronically readable form will be easier and less costly to access ;

— E.F.T. may increase the number of institutions with access to and individual's financial record ;

— On line, real time E.F.T. systems could be used for surveillance, to locate individuals when they conduct a transaction ».

Pour répondre à ces enjeux, il est proposé d'analyser la signification particulière que pourrait avoir l'application des différents principes mis en exergue par la convention du Conseil de l'Europe du 17 septembre 1980. Le choix de cette référence s'explique par le double motif, premièrement, que le Parlement, la Commission et le Conseil des Ministres des Communautés Européennes ont à plusieurs reprises recommandé aux Etats membres des Communautés de ratifier et dès lors de rendre obligatoires les prescrits de la Convention et, secondement, par le fait que la Convention représente dès maintenant un standard minimum commun à partir duquel une réglementation plus ou moins semblable pourrait s'élaborer dans les différents pays des communautés.

L'adoption au niveau européen d'un tel standard, leur ratification et la reconnaissance dans chaque pays de normes équivalentes (ce qui n'est toujours pas le cas en Belgique, Italie, Portugal) permettraient de promouvoir un marché commun des services de télébanking sans crainte majeure pour la « privacy ».

Si les principes de la Convention du Conseil de l'Europe nous serviront de structure pour la seconde partie de la section, nous devrons cependant également tenir compte, dans l'analyse de l'application de chacun des principes, des réglementations ou décisions spécifiques déjà émises dans certains pays à propos des services télématiques voire plus particulièrement des T.E.F.

Quant à la première partie elle sera consacrée à certains principes non directement tirés des réglementations « privacy » mais dont les effets pourraient se cumuler à ceux des réglementations « privacy » pour aboutir à une meilleure protection des données dans le cadre de la réalisation de services T.E.F.

1. Les principes permettant de renforcer l'effet des réglementations « privacy »

Deux principes nous paraissent devoir être évoqués :

— le principe du secret bancaire ;

— le principe du secret des correspondances.

a) Le principe du secret bancaire

Ce principe a été dégagé tant par nos ordres juridiques continentaux que par les juridictions de common law. Des textes pénaux ou constitutionnels le consacrent dans certains pays ; en Europe occidentale, la jurisprudence des Etats européens[2] souligne de

2 Tournier v. National Provincial and Union Bank of England 1 K.B. (1924), 461 ; B.G.H. 4 mars 1979 ; Paris 6 février 1975, D., 1975, 318 ; Cass. b. 25 oct. 1978, J.T., 1979, 371 ; it. 10 juillet 1974, etc.

manière générale l'existence d'une obligation de discrétion du banquier, en vertu de laquelle il engage sa responsabilité contractuelle vis-à-vis des clients et sa responsabilité délictuelle vis-à-vis des tiers. Un courant doctrinal et certaines décisions de justice estiment que cette obligation relève en outre du secret professionnel et serait dès lors pénalement sanctionnée.

Ce secret vise les renseignements confidentiels détenus par la banque y compris les informations relatives aux mouvements de compte et aux opérations effectuées par le client. Par contre, il est d'usage d'admettre la communication à un client d'appréciations générales sur la solvabilité d'un autre client, dans la stricte mesure où le demandeur d'informations justifie d'un intérêt légitime à obtenir de telles informations (MALLMANN, CRADDOCK).

Il est évident que le secret bancaire ou a fortiori l'obligation de discrétion mise à charge du banquier cèdent devant certaines personnes ayant droit à la divulgation du secret (exemple en matière de T.E.F., un autre banquier chargé par le banquier du client d'exécuter l'opération, le banquier du client n'étant pas en mesure de l'exécuter lui-même, ou, autre exemple, le mandataire technique chargé d'acheminer le message électronique). Dans un système électronique de paiement, certaines informations protégées par le secret bancaire sont inévitablement transmises sur des réseaux gérés par des tiers (les mandataires techniques) ; le secret bancaire ne peut avoir pour effet d'empêcher le développement de ces nouveaux modes de transmission à condition, ajoutent certains (SCHWEITZER — MALLMANN), que l'obligation au secret soit étendue à ces mandataires techniques.

Enfin, l'obligation au secret comporte dans tous les pays continentaux des dérogations légales :

1. Le banquier ne peut refuser son témoignage dans une instance pénale et civile en invoquant le secret professionnel.

2. En cas de saisie-arrêt sur le compte d'un client, le banquier tiers saisi ne peut se retrancher derrière la position du client.

3. Il en est de même lorsque le tribunal a besoin d'apprécier la situation économique et financière du débiteur peut prononcer la suspension des poursuites individuelles et l'apurement collectif.

4. L'obligation au secret professionnel cède devant le droit de communication des agents du fisc.

A propos de ces dérogations légales, on note que le Right to financial privacy Act américain de 1978, en réponse aux recommandations de la Privacy Protection Study Commission, impose à l'administration certaines conditions pour accéder aux enregistrements sur des individus ou, ajoute l'Act, sur des sociétés de moins de 5 personnes. L'administration obtiendra l'information soit sur base du consentement écrit du client, soit sur base d'une demande écrite formelle, d'une sommation judiciaire ou administrative ou d'un mandat de recherche. Les mêmes précautions ont été suggérées par l'amendement déposé par les banques canadiennes lors de la révision du Bank Act et finalement non retenues par le gouvernement canadien.

Le texte américain prévoit :

« Notwithstanding any provisions of this or any other Act or Parliament or the legislature of a province, documents or records in the possession of a bank relating to

the affairs of a customer shall not be subject to inspection or seizure under the authority of any statute or regulation or any order, warrant or other process, and premises of a bank shall not be subject to entry and search for such documents or records, unless there shall have been first delivered to the manager or other person in charge of each, branch of the bank from which such documents or records are sought a written demand specifying the customer of the bank in relation to whose affairs the documents are sought and specifying the documents or records required and unless such written demand shall have been issued by a court of competent jurisdiction or by such other authority as may be empowered by statute to authorite such seizure or search ».

b) Le secret de la correspondance

L'utilisation d'un service électronique de paiement doit être considéré comme une correspondance privée et dès lors bénéficier du principe du secret de la correspondance, permet d'affirmer le respect de la confidentialité des messages électroniques en même temps qu'il prescrit le devoir pour les transporteurs de développer des mesures techniques pour assurer une meilleure sécurité des messages.

2. L'application des principes des réglementations « privacy »aux T.E.F.

L'introduction du second chapitre justifiait le choix de la Convention du Conseil de l'Europe pour la protection des données individuelles comme point de départ d'une réflexion sur les mesures spécifiques à prendre en matière de T.E.F. Le chapitre I suggérait la thèse suivant laquelle la spécificité de la réalisation des opérations de T.E.F. exigeait quelques précisions, adaptations voire compléments aux réglementations déjà existantes.

Certaines législations ou décisions nationales ont déjà émis ces précisions, adaptations voire compléments. Leur étude sera proposée en référence aux principes du Conseil de l'Europe.

En suivant la structure même de la convention, le plan de la présente section s'établit comme suit :

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

a) Définitions et champ d'application

Trois définitions méritent d'être analysées, celles de données à caractère personnel, de fichier automatisé et de maître du traitement.

La notion de données à caractère personnel s'entend de données relatives à des individus. On connaît les réticences des législations « privacy » hormis certaines (Autriche,

Luxembourg, Norvège, Danemark, ...) d'étendre la protection des données aux personnes morales. Le projet américain « E.F.T. Privacy Act », analysé par un récent rapport de l'O.T.A. étend sa protection aux petites et moyennes entreprises, au motif que l'utilisation de la carte remise à de telles entreprises peut être considérée indirectement comme faisant naître des données personnelles étant donné le caractère personnalisé de la gestion d'entreprise de cette taille.

La définition de fichier automatisé, telle qu'elle ressort du texte de la Convention et de la plupart des législations nationales, suggère l'existence d'un traitement centralisé facilement localisable. En matière de T.E.F., le fichier de données n'est pas unique mais réparti en de multiples endroits, fichiers locaux sur les T.P.V. ou les G.A.B. fonctionnant en mode local, réseaux avec centres de stockage, centres informatiques bancaires régionaux, etc...

Dans la mesure où la notion de fichier est importante pour permettre aux fichés d'avoir accès à leurs données, « il paraitrait nécessaire d'examiner la nécessité de pouvoir établir l'existence de ce que l'on pourrait nommer un « fichier logique » permettant de situer en dernier ressort, à travers de 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 » (Conseil de l'Europe).

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 la notion de maître du fichier comme « maître du réseau » responsable de l'ensemble des données à caractère personnel reprises dans le réseau ou mieux ce que les travaux du Conseil de l'Europe relatifs à l'impact de la télémétrie, des médias interactifs et des systèmes de courrier électronique qualifient de fichier logique.

L'idée d'un responsable unique vis-à-vis des fiches de l'ensemble des traitements créés par la mise sur pied et la réalisation des services électroniques de paiement et de leur conformité à la réglementation de la protection des données rejoint celle développée par la doctrine et par des organisations internationales (UNCITRAL) à propos des questions de responsabilité civile en cas de non respect des instructions de paiement pour raison d'erreur ou de fraude. Elle s'inspire du même souci de faciliter les recours de l'utilisateur des moyens de paiement électroniques et désigne tout naturellement le banquier ou l'organisme émetteur du moyen de paiement électronique comme responsable pour l'ensemble du réseau.

b) Principes lors de la mise sur pied et de la réalisation des T.E.F.

Les articles 5 à 8 de la Convention du Conseil de l'Europe établissent différents principes, dont seuls certains méritent d'être examinés dans la mesure où les systèmes de T.E.F. obligent à les adapter. Ainsi, le principe de la qualité des données (exactitude, mise à jour) est applicable aux systèmes de T.E.F. de la même manière qu'aux autres traitements. Le propos se limitera aux seuls principes de collecte par des moyens licites et loyaux, à celui de sécurité et enfin au plus important celui de finalité.

— Le principe de la collecte par des moyens licites et loyaux

Le chapitre I insistait sur le fait qu'en matière de services télématiques, les données les plus sensibles sont créées par l'utilisation du service. Cette constatation souligne l'importance de rendre l'utilisateur de ces services conscient des données nominatives qui seront recueillies lors de la réalisation du service et de la finalité de leur enregistrement.

Ainsi, se dégage la double idée d'une transparence pour le fiché des circuits d'information qui permettent la réalisation des T.E.F. et de leur contenu et d'un consentement libre et éclairé du fiché dûment informé, à de tels traitements.

Si le principe du droit d'accès (infra III) nous donnera l'occasion de revenir sur les devoirs d'information qui existent à charge du « maître du réseau », un extrait du rapport de l'O.T.A. souligne l'importance de cette double idée :

« in payment systems, privacy is violated when data are, without the subject's consent, made available to and used by those not a party to the transaction, for purposes other than those necessary to accomplish the transaction. These other purposes could range from organized market campaigns to Government Surveillance or blackmail. If a person has neither explicity nor implicity consented to disclosure and use of information for a given purpose, personal privacy is considered to have been violated even if the same information was willingly provided by that person, either to another party or to the same party for a different purpose ».

— Le principe de sécurité

La particularité des traitements opérés dans le cadre d'un service télématique financier 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 : les 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 d'un service s'engage à prendre toutes les précautions pour que seules les personnes autorisées puissent avoir accès aux informations reprises dans la mémoire[3]. 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'une exigence plus vaste[4] d'une labellisation imposée à tous les centres serveurs offrant des services télématiques « grand public » (les mandataires techniques, en particulier). Cette labellisation s'opérerait sur base d'un plan de sécurité ou d'un cahier des charges défini par des instances normalisatrices au travail desquelles devraient être associées les autorités chargées de la protection des données.

— Le principe de finalité

C'est l'application de ce principe aux traitements opérés par les différents acteurs dans le cadre de T.E.F. qui a suscité le plus de réflexions et d'adaptations. Suivant BAUMANN, commissaire fédéral à la protection des données (cité par GODSCHALK) ce principe prendrait dans le cadre de T.E.F. une triple signification :

3 C.N.I.L., *5° rapport d'activités*, 1985, p. 150.

4 Cf. rapport MONVILLE-POULLET préparé dans le cadre de FAST : La demande finale en télématique - aspects juridiques.

« — So weinig Datenspeicherung wie möglich ;

« — Die Speicherung der für das Bankgeschäft notwendige Daten soll zeitlich begrenzt werden ;

« — Die Datenflüsse sollen so organisiert werden dass dit Transparenz für den Betroffenen maximiert und die Missbrauchsmöglichkeiten minimiert werden ».

Deux des réflexions ainsi proposées s'adressent aux droits et obligations de celui que nous avons qualifié de « maître du réseau », la troisième vise l'application du principe aux transmissions et aux traitements des autres acteurs impliqués dans la réalisation des opérations T.E.F. Nous analyserons séparément ces deux applications.

Le prince de finalité et son application au maître du réseau

L'application du principe aux traitements opérés par le maître du fichier emporte trois conséquences principales :

— la première, relative au contenu des traitements ;

— la deuxième, relative à la durée de la conservation ;

— la troisième, relative aux types de traitements.

i) Le contenu des traitements

L'article 24 (1) de la loi danoise sur les cartes de paiement prévoit :

« 24-(1) Only information on card holders necessary for the carrying out of payment transactions and information on instances where a payment card has disappeared or been revoked due to misuse may be registered ».

Cet article traduit le principe de pertinence (MALLMANN) consacré par les législations notamment allemandes, danoises et autrichiennes, suivant lesquelles seules les données pertinentes, c'est-à-dire celles strictement nécessaires à l'accomplissement de l'opération, objet du contrat conclu avec le fiché, peuvent être enregistrées.

Une recommandation de la N.C.E.F.T. complète de façon heureuse ce principe :

« Governement should minimize the extent to which it requires an institution to maintain and report records about an individual using an E.F.T. system and should minimize the extent to which it requires information to be collected that is not necessary to the operation of the E.F.T. system ».

ii) La durée

L'article 24 (2) de la loi danoise déjà citée contient une prescription relative à la durée, prescription dont l'intérêt est également souligné par la N.C.E.F.T., la commission fédérale suisse de la consommation et le conseil national français du crédit.

« Information on the use of payment systems by individuals and businesses is filed for five years whereupon it is destroyed. However, information on misuse shall be destroyed two years after the registration at the latest ».

On note que les autres sources française et suisse citées à l'alinéa précédent demandent en outre la destruction des renseignements à l'expiration du contrat avec le fiché.

iii) Les types d'utilisation

La recommendation générale de la N.C.E.F.T. américaine servira de base à notre réflexion :

« E.F.T. systems should not be used for surveillance of individuals as to their location or patterns of behaviour ».

On rappellera à dessein, à la suite de la CNIL et du rapport du Conseil National français du Crédit, que la loi française en son article 2 interdit de prendre une décision impliquant une appréciation sur un comportement humain ayant pour seul fondement « un traitement automatique d'informations donnant une définition du profit ou de la personnalité de l'intéressé ». Ce rappel s'adresse tant aux établissements de crédit qu'aux commerçants utilisant les informations créées par l'utilisation du service en vue de la sélection de clientèle (même réflexion de la commission fédérale suisse de la consommation).

Les mêmes recommandations interdisent toute cession (sauf accord exprès du fiché) des informations à des tiers. L'utilisation à des fins de mailing même par l'émetteur de la carte devrait faire l'objet d'une information écrite au client. Ces différents prescrits qui limitent le droit d'utilisation des données du maître du réseau et l'obligent à les rendre transparentes rejoignent le principe qui est à la base de l'article 9 du Bildschirmtextvertrag conclu entre les états fédérés de la République fédérale allemande et réglementant l'offre de services télématiques « grand public ».

Selon ce principe, en matière de services télématiques « grand public », la réglementation doit définir a priori les types d'utilisations autorisées et ce, à l'inverse de ce qui se passe pour la plupart des autres traitements où le principe de pertinence laisse à l'entreprise le soin de définir elle-même ce qui est nécessaire à son fonctionnement sous réserve d'un contrôle a posteriori par les tribunaux ou toute autre autorité (POULLET).

L'article 9 du « Bildschirmtextstaatsvertrag », applicable aux Téléshopping et Télébanking Services limite en effet a priori le type d'utilisation et la durée de conservation des données nominatives créées dans le cadre de l'utilisation des services. Pour être plus précis, l'article 9 al. 3 du Staatsvertrag prescrit que la Bundespost (transporteur et serveur intégré) ne peut traiter que les données nécessaires à la facturation de la communication sans que la durée, la nature, le contenu et le montant de l'opération engagée ne soit reconnaissable et spécifie ce que l'on doit entendre par données nécessaires à la facturation. Le même article interdit à la fois la cession et la constitution d'un profil type par le Bundespost et limite la durée de conservation de ces données au temps nécessaire au recouvrement.

L'alinéa 6 § 2 du même article interdit également au fournisseur de service, la communication et la constitution d'un profil, sauf accord de l'utilisateur. Les entreprises chargées de l'exécution du service sont tenues au même secret (RING-HARSTEIN).

Enfin toujours dans le même esprit, on cite l'article 24 (2) et (3) de la loi danoise :

(2) « Information on card holders may only be used and disclosed when necessary for the carrying out of payment transactions, corrections or legal enforcement, or when authorised by legislation. Information on misuse may only be disclosed to the extent necessary to avoid further misuse ».

(3) « Information on payment creditors may only be used and disclosed when necessary for the carrying out of payment transactions, corrections, and legal enforcement. Information may otherwise only be disclosed to the extent authorised by other legislation ».

Conclusion

Le principe de pertinence mis en évidence par la résolution de la Convention du Conseil de l'Europe (article 5) et à sa suite par certaines réglementations nationales (R.F.A., D.K., en particulier) obligerait le fournisseur de services télébanking à préciser clairement les objectifs légitimes poursuivis par ces traitements, les types d'informations nécessaires pour l'accomplissement de chacune de ces opérations et la durée de conservation de chacune de ces données.

On peut préférer l'approche souple et évolutive que permet ce principe soit à une réglementation a priori des banques de données en fonction du type de données traitées soit à la nécessité d'obtenir une autorisation préalable du fiché ou d'une autorité chargée de la protection des données. L'affirmation du principe de pertinence permet une approche sectorielle qui oblige les associations à définir les finalités de leurs traitements de données nominatives.

A notre avis, l'enregistrement et le stockage des données nominatives nées de l'utilisation du service poursuivent, dans les services de télébanking, comme seules finalités légitimes :

a. l'exécution des ordres de paiement ;

b. la nécessité de conservation des données en cas de recours de l'utilisateur ;

c. la possibilité de procéder à des analyses de marché.

Les autres acteurs impliqués dans la réalisation des opérations

A propos de ces autres acteurs, le projet américain « EFT Privacy Act » introduit la notion d'« EFT Service Provider » c'est-à-dire :

« Any person who provides services including data processing, telecommunications and courier services, intended to accomplish or facilitate, during the period between initiation and completion or a transfer, an electronic fund transfert, but only in regard to the operations of the person in the actual provision of services intended to accomplish or facilitate an electronic fund transfer ».

La notion s'étend donc à tous les intervenants à l'opération y compris le commerçant chez qui le terminal est installé. Elle comprend toute personne qui physiquement participe à l'exécution d'un transfert électronique à l'exclusion du maître du réseau.

D'autres acteurs que le maître du réseau sont en effet impliqués dans la réalisation de l'opération télématique, d'une part, les commerçants détenteurs de T.P.V., d'autre part, les différents intervenants propres au système bancaire dont l'intervention est justifiée par la structure associative (les mandataires techniques) ou réglementaire mise en place.

A propos de ces derniers, la distinction allemande, autrichienne et danoise entre les entreprises travaillant dans le cadre de leurs activités propres et celles traitant de données pour le compte d'autrui permettrait de soumettre à une réglementation plus rigoureuse les services d'exécution technique, les chambres de compensation et les transporteurs, acteurs intervenant dans l'exécution de l'opération sans être parties contractantes à celle-ci.

Ainsi, la jurisprudence allemande à propos de la Schufa, centre de renseignements bancaires mis en place par les banques et délivrant aux seules banques membres des renseignements relatifs à la situation des comptes des clients de ces banques, édicte des principes qui pourraient limiter l'activité de ces mandataires techniques ou institutionnels enregistrant des données pour compte de tiers. La transmission à (an) la Schufa de renseignements nominatifs n'est permise que moyennant accord de l'intéressé. En d'autres termes, les banques ne pourraient constituer un pool de renseignements commun que moyennant l'autorisation de chaque fiché. Par contre, est autorisée la transmission de renseignements par (durch) la Schufa, dans la stricte mesure où cette transmission voire un stockage limité dans le temps et le contenu sont nécessaires aux services mis en place par les banques, services faisant l'objet d'un contrat avec le fiché. La jurisprudence ajoute qu'en aucune manière, la Schufa ne pourrait commercialiser de tels renseignements à des tiers (Mallmann, Moschel).

Dans le même sens, à propos des normes simplifiées n° 12 et 13 adoptées par la CNIL française sur la gestion des comptes bancaires et des contrats de crédit, on notera que si la CNIL (délibérations n° 14 et 15) a du revoir le principe de non communication des données entre banques, principe posé dans la norme initialement définie, elle en a cependant strictement limité l'ampleur et la signification. En effet, elle a permis la diffusion interbancaire de listes noires relatives à la perte, au vol de chèques ou de cartes et aux dépassements de provision mais a réaffirmé qu'elle restait attentive aux conditions de diffusion de l'information et surtout à la durée de leur conservation par chaque institution et surtout par le pool bancaire mis en place pour assurer cette diffusion.

Enfin aux Etats-Unis, est prôné[5] le principe de restriction à la diffusion de l'information même vis-à-vis des mandataires techniques. Les recommandations de la N.C.E.F.T. stipulent :

« There should be no disclosure to private sector without specific authorization by the subject, and certification by the recipient that data will be used only for the designated purpose ;

« Information may be given to support organizations performing routine services for the financial institution, provided it certifies that it will maintain confidentiality ;

« Information may be disclosed to participants and intermediairies to a transaction ; intermediairies include « authorizing/guaranteeing organizations » ;

« Information related to fraud and other crime can be disclosed to law enforcement officers, and customer delinquency can be disclosed to other E.F.T. offerings institutions, credit granting organizations, etc ».

Les commerçants qui disposent de T.P.V. pourraient également trouver bénéfice à obtenir du banquier certaines informations relatives à leur clientèle. Si le secret bancaire est déjà une limite au droit de divulgation de la banque vis-à-vis des commerçants, d'autres plus spécifiques sont invoquées : Schneider estime que le commerçant ne peut avoir accès ni aux listes noires ni à l'état du compte ; le Conseil national français de crédit rappelle à la suite de la CNIL qu'un commerçant qui utilise les informations recueillies dans un T.P.V. de façon nominative, par exemple pour sélectionner sa clientèle, est soumis à la loi Informatique et Libertés et dès lors à déclaration à la

5 Cf. notamment BROWN.

CNIL ; il rappelle en outre l'interdiction de prendre une décision ayant pour seul fondement « un traitement automatisé d'information donnant une définition du profil ou de la personnalité de l'intéressé » (art. 2 de la loi française).

Toujours à propos des commerçants, existe la possibilité pour eux de réaliser les fonctions décrites ci-dessus en ayant un accès direct à une zone de la carte à mémoire. Ainsi, une chaîne de grands magasins pourrait négocier avec une ou plusieurs banques la production de cartes à mémoire où certaines zones seraient réservées à l'inscription de données nécessaires aux commerçants et accessibles que par lui (exemple : les informations relatives au détail de l'opération commerciale). La réalisation de telles cartes à mémoire devrait faire l'objet de conditions inspirées des mêmes principes que ceux évoqués à propos des traitements opérés par le banquier :

1. transparence vis-à-vis du fiché : le fiché doit connaître l'existence de cette zone, quelles données y sont stockées, les personnes qui y ont accès et les buts poursuivis par leur traitement ;

2. limites à l'enregistrement et à l'utilisation de données : le commerçant ne doit traiter les données que pour les besoins légitimes de son commerce, par exemple, peut-être prescrite la nécessité d'anonymiser les données dans le cadre d'analyses portant sur l'évolution du marché de tel ou tel produit, interdite la mention sur la zone de tel ou tel délit (vol dans le magasin, non paiement de marchandises) etc. Le commerçant ne peut céder les données ainsi obtenues et ne peut les conserver au-delà d'une certaine durée.

c) Le droit d'accès du fiché

Par droit d'accès, on entend toute mesure visant à assurer une transparence adéquate des informations et des circuits d'information créés dans le cadre des services de T.E.F.

A cet égard, l'article 13 de la loi danoise sur les cartes de paiement de 1984 est intéressant : certaines informations doivent être données par écrit aux entreprises et individus lors de la demande de délivrance d'une carte de paiement, en particulier, les données personnelles que le porteur de la carte devra divulguer ; l'utilisation, le traitement et la communication des informations personnelles et sur les opérations pratiquées ; les procédures utilisées pour prévenir l'utilisation des cartes disparues ou détenues par des personnes non autorisées.

De même, l'EFT Act de 1978 requérait déjà qu'un client, lorsqu'il signe une convention permettant l'utilisation d'E.F.T., soit pleinement informé à propos de la politique de l'institution financière en ce qui concerne la divulgation des informations nominatives créés par l'utilisation du système ou nécessaires à sa gestion. Une recommandation de la National Commission on E.F.T. établit que « le client doit avoir accès à toutes les données enregistrées et être en mesure de les conteste ».

Certains auteurs (GODSCHALK, SCHNEIDER s'appuyant sur une recommandation de la commission suisse fédérale de la consommation) déduisent du principe de transparence que les informations visibles sur la carte ou communiquées d'une autre manière au détenteur doivent strictement correspondre aux informations enregistrées. Il ne peut être admis que soient introduites dans la carte des informations secrètes et codées inconnues du détenteur (déjà sur ce point, le § 905 de l'E.F.T. Act américain). Cette réflexion vise en particulier les cartes à mémoire qui comme nous l'avons vu peuvent être des cartes à zones multiples dont la lecture peut être réservée ou partagée.

d) Aspects internationaux des T.E.F. et privacy

Dans l'hypothèse de l'utilisation d'un service T.E.F. à partir de l'étranger, se posent des questions de droit international privé qu'il est nécessaire de résoudre. Le fait d'avoir accédé à un service offert par une banque du pays B, à partir d'un terminal situé dans un pays A rend telle la loi du pays A applicable à cette opération ou faut-il appliquer la loi du pays où est situé le « maître du fichier » ? La question peut être plus complexe encore si on relève que le stockage des données ou l'utilisation incriminés ont eu lieu dans un autre pays encore, soit le pays C. Dans le cadre de cet article, nous nous contenterons de renvoyer le lecteur aux nombreux écrits de doctrine écrits sur ce thème relevant notamment la diversité des solutions législatives à ce propos.

Que des règles dites « matérielles » de droit international privé doivent être définies de façon commune à différents pays, est une évidence, les hypothèses relevées étant loin de représenter des hypothèses d'école. Les travaux du Conseil de l'Europe pourraient aider à dégager une solution commune à cet égard. Le caractère international des T.E.F. suggère cependant une autre réflexion plus fondamentale encore.

L'article 12 de la Convention établit le principe de l'interdiction de toute restriction aux flux transfrontières entre pays ayant par la ratification de la Convention des réglementations « équivalentes ». Les recommandations de l'O.C.D.E. souscrivent au même principe.

Il faut bien reconnaître qu'en matière de T.E.F., certaines législations récentes obligent les institutions financières promoteurs de ces services à maintenir les traitements opérés dans le cadre de la réalisation de ces services sur le territoire national. Ainsi, l'article 26 de la loi danoise sur les cartes de paiement stipule :

« Having obtained the opinion of the Data Surveillance Board » (l'organisme chargé du contrôle de la loi danoise de protection des données), « the Ministry of Industry shall make regulations directing that information relative to persons domicilied in the country may only be registered and processed in this country ».

Le Bank Act canadien de 1980 oblige également les banques à opérer les traitements de données relatives à leurs clients domiciliés au Canada sur le territoire national.

On rapprochera ces deux prescrits de l'obligation faite par le Bildschrimtexvertrag allemand aux entreprises offrant des services télématiques sur le territoire allemand, de créer sur ce territoire, une agence qui serait responsable envers les autorités allemandes chargées de la protection des données (RING-HARSTEIN). L'article 45 du projet autrichien relatif au Bildschirmtext de même prévoit l'obligation des serveurs étrangers de suivre les dispositions de la loi autrichienne sur la protection des données.

Ces prescrits s'expliquent certes par la prise de conscience des autorités publiques des dangers particuliers que représente pour la vie privée le développement de ces nouveaux services. Il s'agit pour ces pays de prévenir l'exportation de données nominatives nombreuses et aussi sensibles vers des pays offrant une protection moindre à leurs citoyens. Si cette justification est parfaitement compréhensible, certains craignent que ne s'y ajoutent des motifs de protectionisme économique, tels celui d'obliger les entreprises à traiter les données à l'intérieur du territoire et dès lors concrètement à ne pouvoir offrir des services à l'extérieur de leurs frontières. Or, il est certain que pour le développement des services de T.E.F., la mise en réseau sur une dimension européenne voire mondiale est une nécessité. Pour répondre à cette préoccupation légitime des pays et, dans le

même temps, éviter des réflexes nationaux dictés par des impératifs économiques, il serait utile qu'au sein d'instances internationales, tel le Conseil de l'Europe, en matière de T.E.F. grand public, soient adoptés des standards communs. La définition de ces standards devrait dans toute la mesure du possible s'opérer après consultation de tous les acteurs intéressés : consommateurs, banques et commerçants.

CONCLUSIONS

Du bref survol des réglementations se dégagent certains principes :

— la nécessité de préciser a priori les types d'utilisations pertinentes faites des données nominatives créées par l'utilisation du service et la durée de leur conservation ainsi que l'exclusion de certains types d'utilisation (cession de fichiers à des tiers)[6].

— la reconnaissance d'un droit à l'information élargi pour le consommateur des services de télébanking et de téléshopping, en particulier lors de la demande de la carte ou dès la première utilisation du service.

— la reconnaissance d'un statut particulier pour les entreprises tierces tenues au même devoir professionnel que l'entreprise fournisseur du service[7].

6 Cf. art. 9 Btx-Staatsvertrag et la législation danoise.

7 Cf. en particulier, les diverses banques intervenant dans le règlement d'une transaction ; cf. Projet américain « EFT Privacy Act » et discussion sur les normes de la CNIL.

BIBLIOGRAPHIE

M. B. ELLIS, M. GREGURAS, *The E.F.T. Act*, Prentice Hall éd., New-York, 1983.

CONSEIL NATIONAL DU CRÉDIT, *Rapport juridique sur les aspects juridiques des nouveaux moyens de paiement*, juillet 1986.

C. CRADDOCK, Privacy and Equity in E.F.T.S. : Some basic issues, *The Canadian Banker and ICB Review*.

A. ZAKI, Regulation of E.F.T. : Impact and Legal Issues, *Comm. of the ACM*, Février 1983.

J. SCHNEIDER, Datenschutz und Neue Medien, *N.J.W.*, 1984, 390.

W. BORSUM et V. HOFFMEISTER, *Bildschirmtext und Bankgeschäfte*, doc. polycopié, Institut fur Recht und informatik, Hannover, 1984.

J. LAMBERT, EFT Systems : The Emerging Legal Issues, *The Law Society's Gazette*, 14 novembre 1984.

E. DAUER, *The policy implications of neutral scholarship : a case study of E.F.T. and the Baxter*, Cootner and Scott report, 2, Cardozo L. Rev., 1981, 397 et s.

H. DELAHAIE et A. GRISSONANCHE, *Les nouveaux moyens de paiement. Cahiers de droit*, 1983, 301 et s.

R.C. ZIMMER et TH. EINHORN, *The Law of E.F.T.*, Washington D.C., Card Services, Inc., 1978, 23-31.

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*, 1987, n° 7, 416 et s.

C.E. HELLER, Privacy and the public good, in *Computers and Banking E.F.T., Systems and public Policy*, K.W. Colton and K.L. Kraemer (ed.), New-York, 1982, 82 et s.

O.T.A. *Selected Electronic Funds Transfer Issues : Privacy, Security and Equity*, Background Paper, Congressional Board of the 94 th Congress, 1982.

R. R. TIGERT, *Legal Aspects of E.F.T. in the U.S. Intern. Banking Law*, Feb. 1984, 101 et s.

J.L. BROWN, Implications of the international 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, Jan. 1987.

O. MALLMANN, Datenspeicherung und -ubermittlung, in *Komm. zum B.D.S.G.*, 3° éd., Baden-Baden, Nomos, 1981.

R. SCHWEITZER, La protection des données et autres problèmes juridiques des nouveaux moyens électroniques de paiement, in *Les nouveaux moyens électroniques de paiement*, B. Stauder (éd.), Coll. jurid. romande, Payot, Lausanne, 1986.

T. KAISER, *Legal implications of automated teller machines*, London School of Economics, June, 1985.

D. PARKER, E.F.T. and National Security, *Information Age*, 1982, 19 et s.

C. DUX, Credit Clearing Stellen und Datenschutz, *Datenschutz und Datensicherung*, 1985, 147 et s.

U. DAMMANN, HJ. STANGE, Reform des Datenschutzes imKreditinformationensystem, *Zeitschrift fur Wirtschaftsrecht*, 1986, 486 et s.

A. WESTIN, Privacy issues and the implications of in home banking, *American Banker*, June 3. 1981.

W. MOSCHEL, Dogmatische Strukturen des bargeldlosen Zahlungsverkehrs, *AcP*, 1986, 187 et s.

Les nouveaux moyens de paiement : Droit, Argent et Libertés, Actes du 17° congrès national des huissiers de justice, Dijon, septembre 1986, J.P. FARGET (éd.), Economica, Paris, 1986.

D. FROYSTAD, Data protection in practice : identifying and matching elements, *Teresa* (17), Complex, N.R.C.C.L., Oslo, 1984.