Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur
RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Le transfert électronique de fonds dans ses applications "grand public"

Schauss, Marc; Thunis, Xavier

Publication date:
1987

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Schauss, M & Thunis, X 1987, 'Le transfert électronique de fonds dans ses applications "grand public": problèmes juridiques généraux'.

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

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

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

Download date: 29. Apr. 2025

13

SIXIEME SEMINAIRE EUROPEEN DE DROIT DE LA CONSOMMATION

SIXTH EUROPEAN WORKSHOP ON CONSUMER LAW

CENTRE DE DROIT DE LA CONSOMMATION - UNIVERSITE CATHOLIQUE DE LOUVAIN

ELECTRONIC FUNDS TRANFER SYSTEMS AND CONSUMER PROTECTION

TRANSFERTS ELECTRONIQUES DE FONDS ET PROTECTION DU CONSOMMATEUR

Louvain-la-Neuve, 24-25/09/1987

Le transfert électronique de fonds dans ses applications "Grand Public" : problèmes juridiques généraux

by/par

Marc SCHAUSS
Xavier THUNIS
Assistants au Centre de Recherches Informatique et Droit (C.R.I.D.)
Namur

I. INTRODUCTION

La présente étude vise à une présentation générale des problèmes juridiques posés par les transferts électroniques de fonds. L'approche adoptée sera inductive c'est-à-dire qu'elle partira non pas d'une division abstraite des différentes branches du droit (droit civil, droit des obligations , droit pénal) mais des différentes questions concrètes que pose l'utilisation des transferts électroniques de fonds.

De type inductif, la réflexion sera également une réflexion de droit comparé avec toutes les précautions que ce type d'approche requiert car il faut éviter de transposer purement et simplement des éléments tirés d'un droit étranger qui est censé constituer un système cohérent en lui-même.

L'avantage de notre champ d'investigation est que les développements technologiques en matière de transferts électroniques de fonds sont relativement neufs, uniformes et présentent des aspects internationaux. Dès lors, les différents droits nationaux auront à répondre au même problème fondamental suscité par la dématérialisation des opérations financières ou commerciales lato sensu. Une référence limitée à certains droits étrangers (EU France et Danemark notamment) a donc paru utile pour dégager les éléments d'une éventuelle harmonisation européenne, l'unification du droit matériel ayant une incidence directe sur la solution des problèmes de droit international privé posés par les transferts électroniques de fonds qui ont une vocation internationale et transfrontalière.

Ce caractère transfrontalier s'est affirmé jusqu'à présent surtout dans la télématique professionnelle, dans des réseaux tels que SWIFT, mais il est probable qu'il s'affirmera également à l'avenir dans les réseaux grand-public qui constituent le seul objet de ce rapport [1]. Si les problèmes posés par la télématique professionnelle et la télématique grand-public sont globalement identiques, les solutions à y apporter sont différentes car le poids des partenaires à la transaction, tous professionnels dans un cas, professionnel(s) et "consommateurs" (grand-public) dans l'autre est différent. Une question préalable, délicate à trancher si l'on opte pour une réglementation spécifique est de définir précisement la distinction entre la télématique professionnelle et la télématique grand public plus souvent invoquée que réellement explicitée.

Après une description générale des applications et des précisions terminologiques sur l'ensemble des nouveaux moyens de paiement (II), on définira le transfert électronique de fonds (III) et on exposera les relations contractuelles qu'il présuppose ou qu'il établit entre parties (IV). Des "incidents" peuvent affecter l'opération de transfert électronique de fonds. D'où la nécessité d'examiner les questions de responsabilité (V) et de preuve (VI) ainsi que la révocation d'un transfert erroné ou frauduleux (VII). Les aspects pénaux liés à la fraude dans les transferts font d'ailleurs l'objet d'un examen particulier (VIII) ainsi que les atteintes aux libertés qu'ils peuvent susciter (IX). Les deux derniers chapitres situent le transfert électronique dans le contexte européen. Sont abordés les problèmes liés aux restrictions de la concurrence que peuvent impliquer les ententes entre les différents acteurs du transfert (banques et commerçants) (X). Un aperçu des actions européennes entourant le développement de ces nouveaux moyens de paiement conclut ce travail (XI).

Note de l'introduction

1. Sur les problèmes juridiques posés par les transferts électroniques de fonds entre professionnels, voir B. Amory et X. Thunis, Dématérialisation, authentification et responsabilité, in les transactions internationales assistées par ordinateur, LITEC, 1987, p. 71 et s.

II. LE TRANSFERT ELECTRONIQUE DE FONDS : DESCRIPTION DES APPLICATIONS ET TERMINOLOGIE

1. Description des applications et terminologie

La technique télématique a très vite été adoptée par le monde professionnel pour certaines applications. Celles-ci concernent tantôt les relations interbancaires -on songe aux opérations de compensation (ex. CEC), aux transferts de fonds (ex. SWIFT, CHAPS, SAGITTAIRE) et à la gestion de titres (ex. CEDEL)-, tantôt les relations entre banques et entreprises - fournitures d'informations financières (ex. cours de la bourse ou des devises, simulation de crédit), services de communication (ex. G-Line, Telelink) -.

Les applications à vocation grand-public ont également présenté un intérêt pour les banques. Afin de faire face au problème de l'ouverture aux heures de liberté de la clientèle et de permettre aux employés de banque de concentrer leur activité sur des services personnalisés à la clientèle, les banques ont songé à l'installation de *guichets automatiques*. Ces guichets sont tantôt monofonctionnels (ex. distributeurs de billets (D.A.B) appelés aussi billetteries ; distributeurs d'extraits de compte), tantôt multifonctionnels. Selon les configurations, ils permettent le retrait de billets, le versement d'argent liquide, la consultation du solde des comptes, la commande des formules de virement ou de carnets de chèques, de transférer des sommes d'un compte propre sur un autre compte propre ou encore de s'informer sur le cours des devises. Sauf indication contraire, le présent rapport se limitera aux problèmes juridiques posés par les transferts de fonds. Les terminaux sont installés tantôt à l'extérieur, tantôt à l'intérieur. Ils sont souvent emmurés dans les locaux d'une agence bancaire mais parfois ils le sont dans des endroits publics (ex. gare, hôpitaux, etc...).

L'accès au service par le terminal est subordonné à l'introduction d'une carte magnétique et généralement aussi d'un code confidentiel [1] appelé PIN (Personal Identification Number) ou PIC (Personal Identification Code); parfois, l'accès physique au terminal est subordonné à l'entrée dans un sas qui présuppose l'introduction de la carte dans un lecteur contrôlant

l'ouverture du sas. Cette application met en relation deux parties : la banque et le client.

Une seconde application a connu un développement assez rapide dans certains pays (la Belgique particulièrement). Elle concerne plus spécifiquement le paiement par voie télématique au moyen d'un terminal installé chez le commerçant appelé *terminal point de vente* (T.P.V.) ou terminal de paiement électronique (T.P.E.). Cette application met en relation trois parties : la banque, le client et le commerçant.

Les T.P.V. sont de deux types principaux :

1. apparus plus récemment sur le marché mais d'une technique moins performante, les téléphones dits "intelligents" (Teledata-phone en Belgique), terminaux dont l'appareil de lecture de la carte magnétique est incorporé à un terminal téléphonique relié au réseau commuté à accès public : ils permettent outre la lecture de la carte, la transmission séparée du code secret et l'enregistrement du refus ou de l'autorisation du centre d'ordinateurs. Cette formule présente pour le commerçant, l'avantage du faible coût et les inconvénients de la lenteur, des risques de perturbation et d'un contrôle moins important du bon fonctionnement des terminaux.

2. ceux du second type sont connectés à des lignes louées par le fournisseur du service, c'est-à-dire la banque ou l'association qui gère le service. Le terminal se trouve à l'intérieur des locaux du commerçant ou à l'extérieur.

L'initiative des banques à ce niveau s'explique par le succès du chèque ayant pour conséquence l'émission de nombreux chèques d'un montant trop faible au regard des coûts de traitement.

L'accueil des commerçants vis-à-vis des T.P.V. reste mitigé. Dans leur majorité, ceux-ci y trouvent plus d'inconvénients que d'avantages (coût du terminal, opérations comptables supplémentaires dues à la reconciliation de l'ensemble des transactions). Par contre, les distributeurs de carburant soucieux de valoriser leurs réseaux de distribution en permettant aux clients de s'approvisionner en libre service le soir et la nuit et les grandes surfaces confrontées au problème des files d'attente aux caisses, aggravé

par le paiement par chèque, se sont montrés intéressés par la formule. Sont également intéressées mais dans une moindre mesure, certaines boutiques de produits de luxe qui outre les avantages de la sécurité (réduction des liquidités en caisse diminuant les risques de vol et garantie de bonne fin de l'opération de paiement) et du faible coût de la transaction au regard du prix du produit, voient dans ce service un signe de prestige social .

Outre la demande, d'autres facteurs conditionnent le succès du développement de cette application, notamment la politique des télécommunications. A cet égard, on relève en Belgique, une attitude bienveillante de la Régie des Télégraphes et Téléphones qui a autorisé Bancontact et Mister Cash à exploiter des lignes louées [2]. On note également l'article L. 1071 du Code français des P.T.T. qui autorise l'Administration des Postes à accorder sa garantie aux bénéficiaires de paiement effectuées par les porteurs de cartes de paiement émises par elle.

Le développement des T.P.V. dépend aussi des méthodes de compensation. qui en Belgique ont connu un développement spectaculaire, notamment dans le cadre du CEC (Chambre d'Echange et de Compensation) organisé sous l'égide de la Banque Nationale de Belgique [2bis].
Le T.P.V. est originairement destiné au paiement, mais il permet également d'autres applications, telle la gestion domestique (ex. le relevé mensuel d'achat de carburant qui pourrait être étendu à d'autres produits pour permettre une comptabilité analytique domestique) ce qui, par ailleurs, pose des problèmes de protection de la vie privée.

Une troisième application, la *banque à domicile*, met en relation tantôt deux, tantôt trois parties suivant le service. La banque à domicile ("home banking") consiste en un ensemble de services bancaires variés (situation des comptes, relevé des opérations depuis une date choisie, informations boursières, simulation de crédit, etc...) parmi lesquels les transferts de fonds du compte du client au profit d'un autre compte dont il est titulaire mais aussi des transferts à destination de comptes de tiers (ex. sur Bildschirmtext, service proposé par les caisses d'épargne allemandes ; en France, cette application est proposée par le Crédit Commercial de France et le Crédit du Nord).

L'infrastructure consiste en un terminal d'ordinateur relié au centre d'ordinateurs de la banque par l'intermédiaire du réseau téléphonique commuté d'accès public [3]. Ce type d'application, reste peu développé, notamment pour des raisons de sécurité - souvent le message n'est pas encrypté,- sans doute aussi pour des raisons de politique des services publics : il faut éviter de concurrencer davantage les services financiers fournis par la poste qui relève souvent de la même administration que les télécommunications -. Il rencontre le plus de succès auprès du monde professionnel, particulièrement pour les services de trésorerie, de gestion des comptes et d'informations financières. L'accès à ces services suppose généralement un contrat avec le fournisseur du service (la banque) et le serveur central du système vidéotex aussi appelé intégrateur (l'administration ou l'entreprise de télécommunications)[3bis]. Un code secret est délivré à l'utilisateur.

D'autres mesures de protection existent :
(i) en Allemagne, les transferts de fonds par Bildschirmtext nécessitent non seulement qu'un code secret soit introduit mais aussi un numéro de transaction (Transaktionsnummer ou TAN) valable seulement pour une seule et unique transaction. Une liste de 10 ou 100 TAN est envoyée au client qui le demande. Pour que la transaction puisse avoir lieu, il faut que le TAN corresponde au code secret. Notons que cette solution permet au client de modifier lui-même son code secret quand bon lui semble et ainsi de choisir lui-même son code, ce qui peut être un facteur supplémentaire de sécurité dans la mesure où il fait choix d'un code qu'il mémorise aisément ;
(ii) En France, les transferts ne sont possibles que sur un nombre limité de comptes de tiers préalablement définis de sorte qu'en principe, seuls les transferts ordonnés vers un de ces comptes sont exécutables (il s'agit généralement des fournisseurs réguliers tels que les compagnies d'eau et d'électricité, le bailleur, etc ...). Le code d'accès est composé de 8 caractères alphanumériques dont quatre sont personnalisables et modifiables par le client au moment de l'accès au centre serveur qui calcule au moyen d'un algorithme un autre code de huit caractères validé ensuite par l'utilisateur. En outre, les messages transmis sont chiffrés au moyen d'une clé utilisée pour une transaction ou une tâche donnée (ex. préparation de virement) et modifié ensuite une fois cette transaction ou ce travail exécuté. Enfin, on songe de plus en plus à la carte à mémoire pour ce type d'application.

(iii) une limitation est imposée au montant des transferts possibles. Ainsi par exemple, le service de banque à domicile (voir infra) par téléphone "G-Phone" de la Générale de Banque (Belgique) ne permet de faire des virements à destination de comptes autres que le livret intérêt qu'à concurrence d'un montant de 10.000 francs belges par jour.
Le caractère intégré des systèmes vidéotex dans les pays européens est certainement un facteur de développement de ces services par rapport aux configurations américaines qui rencontrent l'obstacle du manque de standardisation. Remarquons que le système vidéotex utilisant le réseau téléphonique est le plus répandu mais n'est pas le seul envisageable. En Belgique, par exemple, on constate une pression des télédistributeurs en vue d'une valorisation de leurs réseaux par des projets de télématique interactive, notamment de télébanking [4].

Une forme moins élaborée de banque à domicile doit être mentionnée, la "banque à domicile par téléphone" qui existe particulièrement en Espagne (+ ou - 90.000 utilisateurs), en Italie [5], en Belgique et aux Etats-Unis. . Dans ce cas, l'initiation de l'ordre de transfert ne se fait pas au moyen d'un terminal informatique mais au moyen d'un terminal téléphonique multifréquences. Après avoir formé le numéro de téléphone du service, le client est connecté à un ordinateur. Ensuite, il forme son numéro de compte et son code confidentiel au moyen des touches du clavier, après quoi un menu de sélection d'opérations lui est proposé vocalement par l'ordinateur. Le service proposé par certaines institutions financières (ex. Générale de Banque) permet aux utilisateurs de connecter leurs comptes, d'effectuer des virements entre comptes propres (virements internes) ou à destination de compte de tiers (virements externes).

2. Typologie des cartes

La carte constitue aujourd'hui le moyen d' accès aux services de transfert électronique de fonds.
On insiste sur le fait que la carte (accompagnée ou non d'un code d'accès) est un moyen d'authentification parmi d'autres. En effet, le code d'accès seul (ex. plusieurs services de home banking) ou accompagné d'un TAN (ex. transferts de fonds par Bildschirmtext) constitue parfois ce moyen. D'autres solutions ont été imaginées qui sont aujourd'hui à l'état de

prototype ou ne sont utilisées que dans de rares cas et pour d'autres applications que les transferts électroniques de fonds et ce, en raison du coût de ces techniques. On songe ici aux techniques d'authentification par la reconnaissance de caractères physiques tels qu'empreintes digitales, voix, rétine (système utilisé dans certains sites nucléaires), dynamique de l'écriture. Remarquons que certaines de ces techniques n'offrent pas encore toutes les garanties de sécurité. Ainsi, par exemple, les techniques de reconnaissance de la signature présentent un taux de réussite de 90 à 95 %, ce qui est insuffisant. L'utilisation de la carte est la plus répandue actuellement et cette situation est vraisemblablement appelée à perdurer un certain temps.

Les systèmes de cartes sont très variés et assurent des fonctions diverses, parfois totalement étrangères aux services de transfert électronique de fonds. Des précisions terminologiques s'imposent donc afin d'identifier les systèmes de cartes correspondant à la problématique étudiée.

Classifier les cartes et les systèmes de cartes n'est pas chose aisée. Différents critères de distinction s'offrent à celui qui tente pareille entreprise, qui se conjuguent en de multiples combinaisons et dont aucun n'apparaît réellement décisif[6]. On dresse un tableau synoptique des différents types de cartes, que celles-ci concernent les transferts électroniques de fonds ou non.

2.1. Le critère de l'émetteur

On appelle carte *bancaire* la carte émise par une banque ou une institution financière assimilée.
A côté des cartes émises par les banques, existent aussi les cartes émises par des entreprises ou des commerçants ne relevant pas du secteur bancaire. On connaît les cartes émises par des entreprises telles que Diners Club, American Express, DKV, lesquelles permettent d'acquérir des biens chez plusieurs fournisseurs indépendamment de la marque qu'ils représentent ou des produits qu'ils vendent (cartes universelles) et celles émises par un commerçant déterminé (carte *privative* ou carte d'*entreprise* comme par exemple, en Belgique la MAXICARD de GB devenue Shopping Card, la carte Dats de Colruyt ou encore la carte S de Shell, la carte Accord d'Auchan, la carte Pass de Carrefour, ...).

2.2. Le critère de l'utilisateur

Les émetteurs de carte, suivant leur stratégie commerciale visent un certain public : tantôt il s'agira du monde professionnel ou une partie de celui-ci (ex. Carte Euroshell s'adressent plus particulièrement aux transporteurs internationaux), tantôt il s'agira des particuliers ou d'une partie de ceux-ci (ex. American Express).

Dans la présente étude, on se propose d'examiner les applications grand-public en observant que la frontière entre les deux types d'application n'est pas nécessairement rigide.

2.3. Le critère de la fonction

Associée à un titulaire déterminé, la carte assure fondamentalement une fonction d'identification, plus ou moins importante suivant le service. Elle constitue alors une clé d'accès à certains services. Le plus souvent, les cartes sont mixtes, c'est-à-dire qu'elles assurent plusieurs fonctions. Ainsi, la carte bleue en France assure aujourd'hui, outre l'identification, la fonction de carte accréditive, de carte de débit (paiement et retrait) et de carte de crédit réel. On distingue ci-après les fonctions principales des fonctions accessoires.

2.3.1. Fonctions principales

Les cartes servant à certifier dans les succursales d'une banque déterminée que le porteur de la carte est bien titulaire d'un compte auprès de la banque s'appellent *cartes de légitimation*.

Les *cartes de garantie de chèques* (Ex. Carte Eurochèque) confèrent au bénéficiaire une garantie de bonne fin de la banque jusqu'à concurrence d'un certain montant par chèque émis et permettent également de retirer les devises locales dans les agences des banques affiliées. Indirectement: elles participent à la réalisation d'un transfert de fonds dont le départ est l'émission d'un chèque.

Les *cartes de débit* permettent suivant le type de carte, de réaliser

plusieurs des opérations suivantes : retrait d'argent liquide à un guichet automatique de banque (*carte de retrait* appelée aussi *carte de prélèvement*), transfert de fonds de son compte propre sur un autre compte propre et paiement au moyen d'un T.P.V. (*carte de paiement*).

La *carte de crédit* permet au porteur de payer des biens et services avec un certain décalage dans le temps. Le montant maximal à concurrence duquel des achats peuvent être effectués et le délai de paiement sont convenus au préalable. Parmi les cartes de crédit, on distingue la carte accréditive de la carte de crédit sensu stricto [7, 8] :

(i) la carte accréditive autrefois appelée carte de paiement (appellation aujourd'hui réservée aux cartes d'accès aux services de paiement par voie électronique), permet d'acquérir des biens et services auprès de commerçants adhérents au système, lesquels bénéficient d'une garantie de paiement de l'émetteur à concurrence d'un certain montant. Ce type de carte est destiné principalement aux hommes d'affaires et aux particuliers disposant de revenus confortables. Elles sont tantôt nationales (ex. la carte Cofinoga des Nouvelles Galeries en France) ou internationales (ex. Sears).

(ii) la carte de crédit sensu stricto (ou carte de crédit réel ou carte de crédit revolving) offre non seulement le paiement garanti au commerçant mais également, au titulaire, une ligne de crédit d'un certain montant, dans le cadre d'une ouverture de crédit. Ce type de carte est un instrument de crédit et rentre donc dans le champ d'application des réglementations sur les opérations de crédit.

Les cartes de *gestion* se retrouvent essentiellement dans le monde professionnel et plus particulièrement chez les transporteurs routiers qui trouvent dans ce type de carte un moyen efficace et peu onéreux de gérer leur parc de véhicules. Le chauffeur du véhicule qui prélève du carburant introduit une ou deux cartes dans le terminal (dans ce dernier cas, une carte de véhicule et une carte de chauffeur). Les données relatives à la transaction sont enregistrées, traitées et envoyées au transporteur. On rencontre des cartes privatives (ex. carte Texaco) ou universelles (ex. carte DKV), nationales (ex. carte S) ou internationales (ex. carte DKV, carte Euroshell). Ces cartes dont la fonction essentielle est la gestion du parc, assurent également les fonctions accessoires de crédit (le chauffeur

ne paye pas son achat immédiatement mais une facture est envoyée dans un délai convenu soit au transporteur, soit à sa banque en vertu d'un avis de domiciliation) et de ristourne . Elles constituent donc accessoirement des cartes à débit différé.

Les *cartes de ristourne* ou de fidélité donnent à leur titulaire, droit à une ristourne lorsqu'il effectue ses achats chez les commerçants adhérents. On rencontre des cartes de ristourne privatives et non privatives.

Les *cartes préchargées* ou *cartes valeur* (pre-paid store of value) jouent le rôle de jeton , aujourd'hui principalement dans les cabines téléphoniques et les photocopieuses (Telecard en Belgique, Telecarte en France).

Enfin, on connaît les cartes *d'accès aux distributeurs d'extraits de compte*, lesquelles donnent accès à un terminal délivrant, sur demande, des relevés de compte (ex. carte Teles).

2.3.2. Fonctions accessoires

Un même support peut apporter plusieurs avantages qui sont autant de fonctions. Certaines cartes donnent accès, outre aux services pour lesquels elles ont été conçues, à d'autres services. On songe notamment aux services d'*information* (ex. carte Bancontact-Teles qui permet d'obtenir des relevés de compte auprès des terminaux équipés pour cette fonction; carte Bancontact-BBL qui permet la consultation du cours des devises à certains guichets automatiques) et de *commande* de carnets de chèques et de formules de virement. Certaines d'entre elles présentent également des *avantages annexes* tels qu'assurance de voyage, accès à certains clubs, garantie de réservation d'hôtel, facilité de location de voiture, ...) et sont signes de *prestige* social (on pense par exemple aux cartes dites de "prestige" réservées à certaines personnes telle la carte Premier de VISA et la carte Gold de Mastercard). Enfin, dans la mesure où l'accès au compte n'est pas instantané, l'utilisateur bénéficie d'un *crédit* (voyez la note 8).

2.4. Le critère de la technique d'initiation de l'opération

L'initiation d'une opération permise par une carte peut se faire par un procédé électronique ou non.

Lorsque la carte ne sert pas à initier une opération par un procédé électronique, elle est généralement embossée, c'est-à-dire que certaines inscriptions apparaissent en relief et sont pressées sur un papier au moyen d'un appareil appelé dans le jargon "fer à repasser", afin d'établir une facturette signée par le client à des fins probatoires.

Dans certains cas (par exemple en France où les systèmes fonctionnent essentiellement en mode off-line), l'opération est initiée électroniquement par l'utilisateur mais est prolongée immédiatement par une phase manuelle complétant l'initiation électronique, à savoir la signature d'une facturette. Enfin, on connaît les systèmes où l'initiation de l'opération est intégralement dématérialisée (ex.: Mister Cash, Bancontact, Euroshell, Maxicard devenue Shopping ....).

2.5. Le critère de la technique d'exécution de l'opération

Postérieurement à l'acte qui a initié l'opération, l'exécution de l'ordre de transfert peut être réalisée de façon totalement électronique ou au contraire intégrer des étapes d'exécution manuelle ou mécanique. Certains systèmes de carte exigent une initiation mécanique de l'opération trouvant un prolongement informatique (ex. les facturettes établies à partir des cartes embossées qui sont converties auprès d'un centre informatique en bandes magnétiques transmises vers une chambre de compensation). Par contre, dans d'autres systèmes, à une initiation électronique de l'ordre d'exécuter une opération fait suite une exécution non électronique ou partiellement électronique (cfr. transport des bandes à la chambre de compensation). S'agissant des opérations de paiement, on observe que celui-ci suppose parfois une nouvelle action du client, . Ainsi, si l'initiation électronique de la transaction est suivie de l'envoi d'une facture à régler par chèque ou par virement, par exemple, une action nouvelle du client est requise pour réaliser le paiement au contraire de l'hypothèse du paiement par domiciliation (preauthorized payment).

2.6. Le critère de la technique du support

Au niveau technique, le support carte connaît de profondes évolutions. Le premier type de carte n'était absolument pas exploité à des fins de traitement informatique de l'information. Ensuite, des cartes de plastique ont été conçues pour être lues par un dispositif électronique : il s'agit des *cartes à pistes magnétiques* qui représentent aujourd'hui le plus grand nombre de cartes de débit.

Certaines cartes ont également été conçues non seulement pour être lues mais aussi pour qu'à chaque utilisation, des informations puissent y être écrites. Différentes techniques peuvent assurer cette fonctionnalité. Les *cartes à laser* sont actuellement de deux types : la carte holographique utilisée par British Telecom sur laquelle peuvent être enregistrées des unités de communication téléphonique sous forme d'hologrammes au moyen d'un laser et la carte Drexler fabriquée en Drexon sur laquelle des trous de 5 microns de diamètre sont creusés par laser. L'information ainsi générée est lue par un lecteur optique qui mesure l'intensité de lumière réfléchie par le Drexon. Enfin, actuellement, certaines firmes, particulièrement des firmes françaises développent des cartes susceptibles d'être lues, d'être "écrites" mais aussi capables de traiter et de gérer de l'information. Il s'agit des cartes dites *à mémoire*, appelées aussi cartes à puce, à microcircuits, à microprocesseurs, cartes intelligentes ou encore "smart card". On connaît plusieurs versions de ce type de carte. Celles de la première génération permettent outre la fonction jeton (v. supra), de sélectionner les transactions suivant le degré du risque qu'elles représentent, de mémoriser les données relatives aux transactions, de servir de base de données portative, etc.. Celles de la seconde génération (ex. Carte Casio) incorporent non seulement une puce mais aussi les périphériques d'entrée (clavier) et de sortie (écran) et une unité d'accumulation d'énergie (énergie solaire). Il semble que cette dernière technique n'élimine pas les risques de fraude : il serait en effet aisé de réaliser une réplique suffisamment ressemblante permettant de duper le commerçant. Dès lors, il faudrait que cette carte soit certifiée conforme à partir d'un ordinateur central, ce qui ferait réapparaître les risques suscités par les télétransmissions [9].

Pour les besoins de la présente étude, seules les cartes et systèmes de cartes entrant dans le cadre de la problématique des T.E.F. sont retenus, à

savoir ceux qui donnent accès à un service de transfert de fonds. D'où la nécessité de préciser ce qu'on entend par transferts de fonds et plus spécifiquement par transferts électroniques de fonds.

Note du point II

[1] Ce n'est pas toujours le cas. Ainsi, le service TELES qui consiste en la fourniture par un terminal de relevés de compte, ne suppose que la lecture d'une carte d'accès sans la composition d'un code

[2] L'article 86 de l'arrêté ministériel du 20 septembre 1978 dispose que l'abonnement souscrit pour un circuit est personnel et n'a qu'un titulaire. L'acheminement de trafic émanant ou à destination de tiers (comme c'est le cas pour les transferts électroniques de fonds "grand public") est soumis à l'autorisation préalable de la Régie.

[2bis] Pour plus de détails, voir le C.E.C. Continu, Principes de fonctionnement, Association Belge des Banques, Dossier 1, Juillet 1985.

[3] Aux Etats-Unis, l'organisation et l'infrastructure de ce type de service sont différentes.

[3bis] Le "serveur central" ou "intégrateur" est l'organe chargé de gérer l'infrastructure technique centrale du système vidéotex de telle sorte que les communications entre les serveurs externes (par opposition au serveur central) et les utilisateurs se déroulent normalement. Cette fonction est généralement assurée par le transporteur.

[4] PICHAULT, F., "La télématique dans le cadre réglementaire et institutionnel de la Belgique", Courrier hebdomadaire du CRISP, pp. 43-44. Entretien épistolaire avec le secrétaire Général du Conseil National français du Crédit (lettre du 15 décembre 1986).

[5] MITCHELL, J., "Electronic banking and the consumer", International Banking Review, Sterling Publications, London, à paraître ; GONZALEZ, J., "El banco en casa. Les Espagnols prennent la banque à domicile par les cornes", Bancatique, octobre 1986, pp. 478-481 ; PACELLI, V., "Banque à domicile à l'italienne", Bancatique, novembre 1986, pp. 531-533

[6] Pour plus de détails sur les cartes, s'agissant de :

A) Classification et aspects juridiques

Voyez B. SOUSI-ROUBI, Encyclopédie Dalloz, v° carte de crédit, N., Les nouveaux moyens de paiement : Droit, argent et libertés, Economica/ Investir, 1986. N., "Les moyens de paiement sous le signe du plastique", Bulletin hebdomadaire de la Kredietbank, 1er janvier 1982, pp. 1-6, BUYLE, J.P., "La carte de banque à pistes magnétiques", Revue de droit commercial belge, 1984, 658-675, N., Les cartes de paiement (sous la direction de Ch. Gavalda), Economica, Paris, 1980, 113 pages ; N., Les nouveaux moyens

électroniques de paiement, Payot, Lausanne, 1986 et plus particulièrement les Recommandations de la Commission fédérale suisse de la consommation sur la monnaie de plastique, pp. 111-119 ;
RODIERE, R., et RIVES-LANGE, J.C., Droit bancaire, Dalloz, Paris, 3èd. 1980, n°s 198-208 ; GAVALDA, C., STOUFFLET, J., Droit de la banque, PUF, Thémis, Paris, 1974, n°s 601-607, GIGER, H., Kredietkartensysteme, Schulthess Polygraphischer Verlag, Zürich, 1985, 449 p. ; SOUSI-ROUBI, B., Recueil Dalloz Droit commercial, v° carte de crédit

B) Enjeux, stratégie commerciale et prospective

LE TELLIER, H., "Carte de paiement : les enjeux", Sciences et Techniques, octobre 1984, pp. 27-32 ; LE TELLIER, H., "Cartes à mémoire : comment parer la fraude", Sciences et Techniques, juillet 1985, pp. 39-46 ; VAN WYLICK, D., "la puce à l'oseille", Trends Tendances, 2 mai 1986, pp. 37-41 ; N., "Comment paierons-nous demain ?", Trends Tendances, 2 mai 1986, pp. 42-49.

C) Aspects techniques

Mc IVOR, R., "Les cartes à microcircuit", Pour la science, janvier 1986, pp. 58-65 ; MORENO, R., "La carte à microcircuit, premier media à accès logique", Pour la science, janvier 1986, pp. 66-67

D) Application

LE CLECH, Ph., "Cartes à microcircuits : expériences et réalités" Bancatique, octobre 1986, pp. 482-486

[7] On connaît encore un exemple particulier de carte accordant un crédit qui combine l'utilisation d'une carte bancaire (carte de garantie de chèque) et d'une carte privative. La présentation de cette carte par le titulaire qui paye par chèque (appuyé de sa carte de garantie de chèque) donne au titulaire le droit de n'être débité qu'à une date déterminée, date jusqu'à laquelle l'émetteur s'engage à ne pas le mettre en circulation (carte CORA). Aucune opération électronique ne caractérise le transfert de fonds lequel est initié au moyen d'un chèque.

[8] Il est clair que dans les systèmes de carte sans accès au compte, un crédit est accordé au client dans le sens où le débit est différé. Dans ces hypothèses la fonction de crédit est cependant accessoire. Aussi n'intégrera-t-on pas ces cartes dans la catégorie des cartes de crédit.

[9] LE TELLIER, H., "Cartes à mémoire : comment parer à la fraude", o.c., p. 46

III. LE TRANSFERT ELECTRONIQUE DE FONDS : DEFINITION ET QUALIFICATION

1. Définition

Les contours de la notion de transfert électronique de fonds sont peu précis. L'expression est généralement employée tant pour désigner des services de retraits auprès des guichets automatiques de banques que des services de paiement par le biais d'un terminal point de vente (T.P.V.) ou d'un terminal à domicile. On constate donc que l'expression vise aussi bien des opérations totalement électroniques, - paiement par T.P.V. ou banque à domicile (Home Banking) et transfert d'un compte à un autre - que des opérations semi-électroniques, telles que des transferts dont seul le traitement est réalisé par des procédés informatiques (Ex : non échange de chèques).

Le transfert électronique de fonds se distingue des formes traditionnelles fiduciaires ou scripturales par le fait que ne sont utilisés ni des espèces ni des instruments de paiement papier mais uniquement des impulsions électriques émanant d'un donneur d'ordre qui s'est identifié pendant la procédure d'accès prescrite[1]. Le point essentiel est l'exclusion de l'utilisation d'un instrument de papier (Ex. chèque, virement ....) lors de la création ou de l'engendrement de l'acte de transfert de fonds. Ce critère est important car il permet d'écarter de la qualification de transfert électronique les opérations dont seul le traitement mais non l'initiation s'effectue par des moyens électroniques (v. infra).

En droit, deux possibilités sont ouvertes : ou la réalité technologique en question, à savoir le transfert électronique de fonds peut se rapporter à un concept connu, ou le législateur doit créer un concept nouveau susceptible de combler le "vide juridique" engendré par l'irruption d'une technologie nouvelle. C'est cette seconde perspective qu'a adoptée le législateur américain en promulguant l'"Electronic Fund Transfer Act" (E.F.T.A.), réglementation fédérale américaine complétée par la Regulation E entrée en vigueur le 10 mai 1980. Quels sont les éléments que le législateur fédéral américain a retenus comme pertinents pour définir le transfert électronique de fonds ?

La définition adoptée dans l'EFTA est la suivante : " Any transfer of funds other than a transaction originated by check, draft or similar-paper instrument, that is initiated through an electronic terminal, telephone, or computer or magnetic tape for the purpose of ordering, instructing or authorizing a financial institution to debit or credit an account". L'approche américaine retient donc comme critère le caractère électronique ou non du moment initial du transfert de fonds.

Précision supplémentaire, l'EFTA ne s'applique que pour autant que dans l'opération de transfert de fonds soit impliqué un compte détenu par un consommateur. La notion de consommateur est difficile à cerner et la définition donnée par le législateur américain en est pour le moins laconique [2].

Bien que plus liée à un support spécifique, la loi danoise sur les cartes de paiement, entrée en vigueur le 1er janvier 1985, semble de portée plus générale que l'EFTA quant à son champ d'application ratione personae. Selon l'article 1, "The Act applies to payment systems with payment cards and to similar payment systems which are offered to the public (nous soulignons)... "L'article 13 confirme cette impression puisqu'il indique :"When approaching individuals and businesses ....(nous soulignons)".

Concrètement, quels types de transfert électronique de fonds "grand-public" recouvre la loi américaine ?[3].

1. Les distributeurs automatiques de billets (D.A.B.) par lesquels sont exécutées, au moyen d'appareils électroniques, diverses opérations de transferts de fonds ou encore de transmissions d'informations par voie électronique.
2. Les terminaux point de vente (T.P.V. ou encore Point of Sales Terminals) qui permettent au consommateur de régler par voie électronique achat de biens ou prestations de services notamment dans les grands magasins ou les stations services.
3. Les paiements par téléphone en connection directe avec le centre d'ordinateurs de l'organisme financier intéressé ou du système électronique. Cette forme de paiement apparemment fréquente aux Etats-Unis semble plus rare en Europe et implique de toute façon que le client observe minutieusement la procédure d'accès prescrite[4].

Les trois formes de transferts décrites ci-dessus sont électroniques.

L'EFTA couvre bien d'autres formes de transferts considérées comme électroniques : ainsi, les "preauthorized payments" qui correspondent aux instructions permanentes de paiement et aux domiciliations couramment pratiquées en Belgique. Cette quatrième forme ne fait pas l'objet de la présente étude [5].
Par ailleurs, ne rentrent pas dans le concept de transfert électronique de fonds ni le paiement par carte préchargée car celle-ci ne donne pas lieu à une inscription en compte ni la technique du non-échange de chèques ou de virements parce qu'à l'origine des opérations ainsi traitées réside un écrit signé par le donneur d'ordre ou le tireur. Seules les données sont traitées et échangées par voie électronique ou télématique.

Enfin, nous écartons du concept de transfert électronique de fonds "grand-public" les virements avec support mécanographique (V.S.M.), forme de transferts s'adressant spécifiquement aux entreprises. Les entreprises disposant de leur propre service de traitement de l'information peuvent substituer aux formules de virements des supports mécanographiques standardisés, telles des bandes magnétiques qui sont traitées par le centre d'ordinateurs de leur banque.

2. Essai de qualification

Note préalable : le transfert électronique de fonds : une nouvelle forme de monnaie ?
Comme des moyens électroniques permettent d'initier le mouvement de fonds, d'aucuns ont parlé d'une nouvelle génération de monnaie, la monnaie électronique. L'expression de "monnaie électronique", quoique séduisante par le parallèle qu'elle trace avec la monnaie fiduciaire et la monnaie scripturale, semble erronée. Même si le mode de déclenchement du transfert est électronique, ce qui est déclenché est une inscription en compte. Il serait donc plus exact de parler de monnaie scripturale gérée électroniquement (M. VASSEUR).

Sur le plan technique, rien ne distingue le transfert électronique de fonds de la transmission par télécommunication de n'importe quelle autre information. Il s'agit d'un message particulier indiquant le compte débiteur, le compte créditeur et le montant à transférer qui, encodé,

circule sous forme de signaux sur les réseaux de télécommunications. Il y va donc simplement d'un transfert télématique d'ordre de paiement, la télématique constituant un nouveau vecteur de la monnaie scripturale.

La figure juridique la plus souvent utilisée pour qualifier le transfert est incontestablement le virement. Ce qui permet à la doctrine dominante d'en déduire des conséquences quant au moment du paiement et aux questions corollaires relatives par exemple à la révocation de l'ordre de paiement. La portée et l'utilité de cette analyse doivent être soigneusement cernées.

La portée, tout d'abord. Le virement ne saurait qualifier le retrait ou le versement d'argent liquide à un distributeur automatique de billets. Par contre, l'analyse pourrait s'avérer adéquate pour qualifier le transfert électronique initié par le client au départ d'un terminal point de vente pour apurer la dette qu'il a vis-à-vis d'un commerçant en suite à la conclusion d'un contrat de vente de biens ou de prestation de services.

L'utilité de l'analyse ensuite. La nature juridique du virement est assez incertaine. S'agit-il d'une délégation, d'un mandat ou d'une exécution de contrat ? Il ne peut s'agir d'une délégation car le caractère novateur de celle-ci impliquerait que la banque devienne le débiteur du bénéficiaire, ce qui n'est pas le cas.
La qualification de mandat fait également problème car le mandat porte, en droit belge et français tout au moins, sur des actes juridiques et il n'est pas sûr que le transfert de fonds, réalisé par un jeu d'écritures comptables ou autrement, constitue un acte juridique.

Si l'on tient à l'expression "virement électronique", c'est l'analyse du virement retenu par messieurs Van Rijn et Heenen [6] qui s'avère à notre avis la plus convaincante et la plus utile en notre matière car elle permettra de préciser en quoi consiste selon nous le transfert électronique de fonds. "Le virement n'est ni une opération purement consensuelle ni un contrat, il constitue un mode d'exécution de deux contrats préexistants, le dépôt de fonds ou ouverture de crédit et la convention entre le donneur d'ordre et le bénéficiaire". "En réalité, qu'il s'agisse de retrait au départ d'un distributeur automatique de billets ou qu'il s'agisse d'un transfert initié au départ d'un terminal point de vente, le transfert électronique de fonds constitue pour le client un mode supplémentaire de mobilisation des fonds qu'il a déposés ou de crédit que

lui a octroyé le banquier. Celui-ci en mettant à la disposition du client un appareil en ordre de marche et en s'étant accordé avec le commerçant pour l'installation d'un terminal point de vente ne fait qu'exécuter son obligation née du contrat de services, accessoire au dépôt ou à l'ouverture de crédit, par lequel le banquier permet à son client de bénéficier moyennant rémunération d'une modalité (électronique) de mobilisation des fonds inscrits en compte. Chaque fois que le client utilise le service offert, il profite d'une facilité prévue par le contrat et d'une technique d'exécution nouvelle d'une opération bancaire traditionnelle tendant le plus souvent au paiement d'une dette préexistante (sous réserve de l'hypothèse particulière d'une donation)[7].

Il n'y a donc pas à chaque fois, entre la banque et le client, un nouveau contrat mais une répétition d'actes d'exécution d'un contrat de services déployant ses effets dans la durée. Nous préciserons par la suite les effets de cette conception notamment en matière de preuve des opérations passées.

L'expression "technique d'exécution nouvelle des opérations bancaires traditionnelles" rend assez bien compte du type de problème juridique que peuvent poser les transferts électroniques de fonds. D'une part, des problèmes juridiques classiques sont réactivés tels que par exemple le moment du paiement, la fraude, la responsabilité des parties. D'autre part, des problèmes nouveaux surgissent, issus de la dématérialisation des opérations bancaires et spécifiques à cette dématérialisation. On songe ici essentiellement au problème de preuve.

Notes du point III

[1] D. SYX, Aspects juridiques du mouvement électronique de fonds, Kredietbank, 1982, P. 12 et s, Voir aussi E. BERGSTEN, Electronic banking : the legal framework, Brussels, 9-10 march 1987.

[2] L'article 205.2 (e) de la Régulation E (12 CFR 205) indique "consumer means a natural person".

[3] Voir D. Syx, op. cit., p. 15.

[4] Pour plus de détails, M. ELLIS et F. GREGURAS, The Electronic Fund Transfer Act and Federal Reserve Board Regulation E, Prentice Hall 1983, p. 37.

[5] Pour plus de détails, M. ELLIS et F. GREGURAS, op. cit., p. 97 et s. Certes, le compte d'un consommateur est bien impliqué par ce type de transfert mais peut-on soutenir pour autant que le consommateur lui-même initie électroniquement l'opération, cfr. sur ce point M. ELLIS et F. GREGURAS, op.cit., p. 23 et s.
Sur les dangers des "débits préautorisés", N. LHEUREUX, Les effets de la technologie et la protection des droits des consommateurs dans le paiement bancaire, Les cahiers de droit, 1983, p. 263 et s.

[6] VAN RYN et HEENEN., Principes de droit commercial, Bruylant 1960, T. IV, n° 2059

7 Pour plus de détails Y. POULLET et X. THUNIS, réflexions sur le mouvement électronique de fonds in La Télématique, Aspects techniques, juridiques et socio-politiques, T. II, Story-Scientia, p. 257 et s.

IV LE TRANSFERT ELECTRONIQUE DE FONDS : LES RELATIONS CONTRACTUELLES ENTRE PARTIES

1. L'aménagement des relations contractuelles dans le transfert électronique de fonds

Les services de transferts électroniques de fonds ou de télématique bancaire consistent essentiellement en l'exécution d'un ou de plusieurs contrat(s) situé(s) en amont de l'opération de transfert. Une convention entre le fournisseur du service et l'utilisateur aménage les relations concernant la gestion et l'utilisation de ce service.

L'aménagement contractuel du service de transfert électronique de fonds diffère suivant le type de service. Nous distinguons ci-après les services effectués au moyen d'un guichet automatique (G.A.B. ou A.T.M.), d'un terminal point de vente (T.P.V. ou P.O.S.) et le service de banque à domicile lequel est réalisé tantôt par videotext (pays européens) tantôt par des moyens analogues mais ne présentant ni la même structure ni la même organisation (Etats-Unis).

1.1. Les guichets automatiques de banque [1]

Il s'agit ici d'une relation bilatérale par terminal interposé entre la banque et son client. Des transferts de fonds par le biais de ces guichets supposent que le client bénéficie auprès de son banquier d'une ouverture de crédit ou qu'il ait conclu avec celui-ci un contrat de dépôt de fonds. Deux conventions lient donc la banque et son client : un dépôt ou une ouverture de crédit et un contrat de services accessoire au premier, contrat par lequel la banque permet à son client de bénéficier moyennant rémunération d'une modalité (électronique) de mobilisation des fonds inscrits en compte. Le tout se fait le plus souvent grâce à la combinaison d'une carte et d'un code d'accès.

On pourrait envisager à l'avenir que la relation actuellement bilatérale devienne triangulaire dans la mesure où les services accessibles aux guichets automatiques pourraient permettre par exemple de transférer des

fonds du compte d'une personne au compte d'une autre personne. On pourrait aussi imaginer que l'utilisation des guichets soit ouverte à des personnes qui ne sont pas liées à la banque par une convention préalable.

1.2. Les terminaux points de vente

Les transferts de fonds réalisés par les terminaux points de vente mettent trois personnes au minimum en relation : le client, la banque et une tierce partie bénéficiaire, à savoir un commerçant. L'opération de transfert électronique de fonds par terminal point de vente suppose i) l'existence d'une convention de dépôt ou d'ouverture de crédit entre le client et la banque, ii) l'adhésion du client à la convention de services par laquelle la banque met à sa disposition des moyens électroniques de mobilisation des fonds inscrits en compte, iii) une convention entre le commerçant et la banque portant sur l'installation du terminal point de vente et sur l'acceptation par le commerçant des paiements effectués par ce biais, iv) une convention entre le commerçant et le client que ce dernier doit exécuter (payer au sens juridique du terme).

1.3. la banque à domicile (home banking)

Les opérations de banque à domicile peuvent impliquer une relation tantôt bilatérale, tantôt triangulaire. Le service peut consister en une simple relation entre le banquier et le client (ex. transfert par le client d'un compte à vue vers un compte d'épargne logement) ou en payement à un tiers. Le scénario contractuel sera identique tantôt à celui qui caractérise les opérations à un guichet automatique tantôt à celui qui caractérise les opérations par terminal point de vente à la différence près qu'une convention lie l'utilisateur et une administration (ou une entreprise privée) de télécommunications portant sur l'utilisation de l'infrastructure intégrée du système vidéotext (serveur central ou intégrateur).

Conclusion : Quelle que soit l'hypothèse envisagée, guichet automatique de banque, terminal point de vente ou banque à domicile, l'accès aux services de transferts électroniques de fonds est subordonné à la conclusion d'un contrat réglementant leur utilisation.

2. Analyse sommaire de la convention "transfert électronique de fonds"

2.1. Parties à la convention

De multiples acteurs sont impliqués dans l'exécution du service et tous ne sont pas en relation contractuelle avec l'utilisateur (ex. banque du bénéficiaire, chambre de compensation, propriétaire du terminal, propriétaire du lieu où est situé le terminal dans le cas du paiement électronique, organisme gestionnaire du réseau ....).

2.2. Aspects abordés par la convention

Les conventions de services "transfert électronique de fonds" précisent généralement l'objet du contrat, les modalités de délivrance de la carte et du code secret, les obligations du client relativement au code, la procédure d'opposition en cas de perte ou de vol de la carte et ses effets, les responsabilités des parties, le régime de la preuve des opérations, l'information de l'utilisateur par la banque (relevés de compte et tickets), la durée de validité du contrat ou de la carte, la procédure de modification du contrat, le coût du service et le régime des informations détenues par le fournisseur du service ; éventuellement le contrat contient une clause de juridiction. La plupart de ces problèmes seront réexaminés dans la suite de l'exposé.

2.3. Qualification de la convention

Etant donné la relation de confiance et le contexte de crédit dans lequel s'inscrit l'octroi de moyens d'accès, il semble que la convention soit une convention "intuitu personae".

Le client introduit une demande qui est acceptée ou non par l'institution financière. Le refus de celle-ci peut s'expliquer par exemple par la garantie que l'émetteur assume vis-à-vis du commerçant ou en raison d'usages frauduleux antérieurs par le client. Les contrats prévoient très généralement qu'en tout cas l'octroi de la carte est laissé à l'appréciation discrétionnaire de l'institution financière. Il en résulte qu'elle est libre de ne pas contracter avec telle ou telle personne [2].

La convention se qualifie en un contrat d'entreprise mettant à disposition du client un certain nombre de services susceptibles de permettre la réalisation de l'opération de transfert électronique de fonds.

Autre caractéritique : il s'agit d'un contrat d'adhésion dont le caractère standard s'explique partiellement par la nécessaire cohérence du système du moins au point de vue technique (voir infra). Certaines clauses sont parfois considérées comme inéquitables ou déséquilibrées et d'aucuns ont souhaité une intervention réglementaire directe afin de les rééquilibrer. Ce point sera repris ultérieurement.

Comme on l'a indiqué plus haut, deux Etats ont jusqu'à présent édicté une réglementation concernant directement ou indirectement le transfert électronique de fonds. Ce sont les Etats-Unis et le Danemark. Les dispositions de ces deux législations, d'optique assez différente puisque la loi américaine prend en considération les transferts électroniques de fonds alors que la loi danoise prend en considération les services bancaires de paiement au moyen de cartes constituent un précédent intéressant et seront fréquemment citées dans la suite de l'exposé traitant de la responsabilité, de la preuve des opérations effectuées et du règlement des conflits.

Notes du point IV

[1] Sur ce qui suit, voir Y. POULLET et X. THUNIS, op. cit., p. 258 et s. Voir aussi J. HUET Dossier monétique : relations entre établissements financiers, commerçants et porteurs de cartes de paiement (France), Droit de l'informatique, n° 86/3, p. 117 et s.

[2] Bien que la nature "quasi publique" du service rendu par le banquier soit aujourd'hui mise en évidence, on considère généralement que le banquier est libre d'accepter ou non l'ouverture d'un compte, sous réserve d'un refus abusif. La solution a été transposée contractuellement à la délivrance des moyens d'accès.

Comp. cependant la situation en France où le droit à la disposition d'un compte bancaire a été instauré par l'article 58 de la loi du 24 janvier 1984. Pour plus de détails, L. SIMONT et A. BRUYNEEL chr. de droit bancaire privé. Les opérations de banque (1979-1985), Rev. de la Banque, 1987, n° 6, p. 32.

V. QUESTIONS DE RESPONSABILITE

D'entrée de jeu, on se doit de souligner que si les questions de responsabilité et de preuve sont traitées séparément des questions de preuve, les deux problématiques sont intimement liées, la preuve d'un droit étant la condition de son exercice et réagissant donc sur le fond même du droit. Afin de poser correctement les questions de responsabilité, il paraît indispensable d'identifier les risques et les dommages possibles dans une opération de transfert électronique de fonds (1). On examinera ensuite les questions de responsabilité relatives à la distribution des moyens d'accès (2) de même que celles liées à la garde et à l'utilisation de ces moyens d'accès en envisageant les obligations respectives de l'utilisateur, de la banque et, le cas échéant, du commerçant dans le cas des terminaux points de vente (3) et (4). On tire enfin les conclusions des diverses considérations émises; des pistes de réflexion seront également évoquées (5).

1. Le transfert électronique de fonds : identification des risques et des dommages possibles

1.1. Les risques

Il existe *un risque quant à l'identité de l'émetteur de l'instruction* suite à une erreur d'authentification de la personne autorisée à accéder au système, ou à une fraude ; celle-ci se matérialise par exemple par une duplication de cartes ou la création d'autres cartes d'accès, par la technique dite du "buffering" qui consiste à modifier les informations stockées sur la piste magnétique de la carte ou encore par la découverte du code secret. Il est certain que ce risque est très faible lorsque l'authentification se fait au moyen de techniques plus fiables telle la reconnaissance électronique de caractéristiques personnelles (ex. pupille de l'oeil, empreinte digitale, pavillons d'oreille, dynamique de l'écriture, ...). La carte à microcircuits diminue aussi les risques liés à l'accès dans la mesure où la percée du code secret est quasi-impossible de même que la falsification de la carte. En effet, une des techniques pour percer le code secret consiste à l'intercepter durant son transport vers l'unité centrale.

Or, la carte à microcircuits supprime ces transferts d'information sur les lignes de télécommunications auxquelles il est relativement aisé de se connecter.

Un deuxième type de *risque* est celui de l'*altération du message* qui peut se produire en tout point du transport du message. Les causes peuvent être une erreur de programmation (ex. erreur dans le système d'exploitation, erreur dans les protocoles ou démagnétisation) ou une intervention humaine (fraude). L'altération peut porter sur le montant transféré ou encore sur le destinataire de la prestation.

Un *retard* dans l'acheminement du message et dans l'exécution des instructions y contenues peut être dû à un encombrement des lignes de télécommunications, à des coupures de courant, à une stratégie du gérant du système (ex. banque qui "gèle" l'exécution de l'odre de virement), à certaines caractéristiques techniques (ex. systèmes off-line) ou encore à l'intervention frauduleuse d'un tiers.

Enfin, le message peut se *perdre* en cours de route par exemple à cause d'une démagnétisation des supports d'information due à une catastrophe naturelle (ex. foudre), à cause d'une erreur de programmation ou la destruction du support assurant le transport. La trace de l'opération réalisée peut également être perdue a posteriori (perte ou destruction des mémoires auxiliaires).

Différents *facteurs de risques* concourrent à la réalisation d'incidents. D'abord, la technique téléinformatique n'est pas encore arrivée à maturité. Un deuxième facteur réside dans l'obsolescence de certains équipements (particulièrement ceux des administrations de télécommunications) au regard des services mis en oeuvre. La délinquance ou plus exactement la fraude informatique (car la plupart des agissements de fraude ne constituent pas des délits) est un troisième facteur entretenant sans doute un lien avec les deux premiers. Enfin, la multiplicité des intervenants à l'opération (tant dans l'aspect matériel qu'humain) et l'absence de standardisation des équipements et de la forme des messages sont également des facteurs de risques.

La multiplicité des intervenants pose de difficiles questions de recours sur le plan juridique. Le schéma peut être très complexe pour ce qui est

des services interbancaires. Interviennent le donneur d'ordre, la banque du donneur d'ordre, la banque du bénéficiaire, le bénéficiaire (p. ex le commerçant dans l'hypothèse d'un terminal point de vente) éventuellement une ou plusieurs banques correspondantes, la ou les chambres de compensation, le transporteur et l'utilisateur, et éventuellement un "mandataire" technique.

Sur le plan juridique, il faudra vérifier si la théorie classique de la responsabilité confrontée à une pluralité d'acteurs et à la rapidité dans la transmission d'informations dématérialisées se révèle toujours adéquate. En effet, sa mise en oeuvre suppose que soient établis un dommage et un fait fautif qui en soit la cause. Si le dommage est généralement aisé à établir (même s'il est quelquefois difficile à localiser) il n'en va pas de même de la faute et de la relation causale avec le dommage.

1.2. Le dommage

Les incidents dans le transfert électronique de fonds peuvent entraîner différents types de pertes : perte du *principal*, perte des *intérêts*, perte due à une *variation du taux de change*, dommages "*dérivés*". Ils peuvent également constituer une *atteinte à la vie privée*.

La perte du *montant* ou d'une partie de celui-ci se produit lorsque l'ordre de transfert a été mal exécuté, créditant le compte d'un bénéficiaire erroné ou débitant le compte d'une personne étrangère à l'opération au lieu de débiter le compte du donneur d'ordre. Il n'y a pas de problème si une régularisation peut intervenir avant que le bénéficiaire erroné n'ait utilisé les fonds dont son compte a été indûment crédité.

En cas de paiement tardif, les *intérêts* de la somme sont perdus tantôt pour le donneur d'ordre, tantôt pour le bénéficiaire. Un problème important du point de vue du donneur d'ordre est de déterminer le délai d'exécution de l'ordre de transfert.

Ce même problème se pose s'agissant de pertes résultant de *variations du taux de change*.

Le retard dans l'exécution de l'ordre de transfert peut également entraîner *d'autres dommages*. Pour le donneur d'ordre par exemple qui, du fait du

retard, n'a pas satisfait à ses obligations contractuelles ou légales, et doit payer des dommages et intérêts moratoires , supporter une clause pénale, ou encore une amende. Le bénéficiaire peut par suite du retard, encourir les mêmes dommages que le donneur d'ordre. Il peut ainsi, vu l'absence des liquidités au moment escompté, avoir laissé échapper un marché, subir la résiliation d'un contrat important, ou se voir contraint de trouver des alternatives de financement plus onéreuses. Le problème délicat en droit sera de qualifier ces dommages "dérivés" en dommages directs ou indirects c'est-à-dire d'examiner s'ils entretiennent un lien suffisamment intense avec la faute d'un des intervenants pour donner lieu à réparation.

Enfin, les transferts électroniques de fonds peuvent engendrer des dommages extra-patrimoniaux. On songe ici aux *atteintes à la vie privée* (v.infra).

Pour le grand public, ce sont surtout les pertes du montant principal qui sont les plus préoccupantes. On ne négligera cependant pas les pertes d'intérêts bancaires et les pertes dues aux fluctuations du taux de change ; certes d'un point de vue individuel, elles ne devraient pas représenter de fortes sommes, les retards dans l'exécution des transferts étant généralement limités et les sommes en cause le plus souvent peu importantes. Il n'en reste pas moins, que les transferts grand public peuvent porter sur des sommes élevées, et les variations du taux de change s'avérer importantes ; et surtout, mêmes minimes individuellement, les préjudices cumulés peuvent aboutir à un préjudice collectif important pour les utilisateurs. Ceci pose la question, souvent débattue, du recours des utilisateurs à titre individuel ou collectif et en définitive du droit d'accès à la justice.

2. Questions de responsabilité relatives à la distribution des moyens d'accès (carte et/ou code d'accès)

Comme le montre l'espèce suivante, des risques d'utilisation abusive des moyens d'accès existent avant même que le consommateur n'ait pu recevoir et utiliser lui-même ces moyens d'accès. Une dame invalide avait reçu par la poste une carte bancaire qu'elle n'avait pas sollicitée accompagnée d'une demande pour un P.I.N. (Personal Identification Number). La dame avait demandé à son concierge de détruire la carte mais celui-ci l'avait

cependant conservée, renvoyant à la banque une demande contrefaite pour obtenir un P.I.N. Après avoir reçu le code en question, le concierge avait fait plusieurs retraits et les avait imputés au compte de sa patronne. (1) Cet exemple soulève deux questions distinctes 1° la charge des risques liés à la délivrance des moyens d'accès (carte ou code) par un mode de transmission donné (ex : la poste), risques qui naissent de l'interception par des tiers 2° l'envoi de produits ou de services non sollicités par l'utilisateur.

On répond comme suit à ces questions
1° on peut laisser aux banques le soin d'apprécier le risque lié à l'interception des moyens d'accès aux distributeurs automatiques de billets ou aux terminaux points de vente. Selon nous, l'élément essentiel qui doit ici guider l'analyse est que le consommateur titulaire de la carte ne soit pas tenu pour des transactions effectuées avant d'avoir reçu effectivement ces moyens d'accès.

En pratique, plusieurs solutions sont envisageables. Il faut éviter l'envoi concomitant par la poste de la carte et du code d'accès permettant les débits en question. La formule suivante, déjà d'ailleurs partiellement appliquée en Belgique, pourrait être envisagée : le client vient directement chercher sa carte auprès de l'organisme bancaire, le code confidentiel d'identification étant envoyé par la banque sous pli recommandé avec accusé de réception.

2° concernant l'envoi non sollicité de moyens d'accès, l'Electronic Fund Transfer Act" américain pose en règle générale (15 US C 1693 a 903 1) qu'un organisme financier ne peut mettre à la disposition d'un client des moyens d'accès que si le client lui-même en a fait la demande par écrit ou oralement ou pour renouveler ou remplacer des moyens d'accès attribués précedemment au client. Cette règle vise à combattre la pratique, apparemment répandue en Amérique, d'envois automatiques de cartes en l'absence de demande du consommateur.

L'article 14.1. de la loi danoise se prononce dans le même sens et dispose : "Payment cards shall only be furnished upon application"
Il va sans dire que l'organisme financier doit supporter toutes les conséquences dommageables dérivant de l'inobservation de l'interdiction.

3. Questions de responsabilité liées à la garde et à l'utilisation des moyens d'accès : obligations respectives de l'utilisateur, de la banque et du commerçant (dans le cas d'un terminal point de vente).

Comme on l'a relevé plus haut, l'utilisation de moyens d'accès aux transferts électroniques de fonds comporte des risques, risques essentiellement de débits illicites, notion difficile à définir dont on pourrait dire sommairement qu'elle consiste en débits non-autorisés soit par la banque qui délivre les moyens d'accès, soit par le client qui en est le titulaire. L'analyse implique des aspects pénaux que nous n'aborderons pas dans ce chapitre et que nous reportons dans l'étude de la fraude.

3.1. Les hypothèses de débit illicites

La jurisprudence et la majorité de la doctrine se sont, jusqu'ici, concentrées sur les débits illicites pratiqués à partir des distributeurs automatiques de billets (D.A.B.). L'analyse peut, sans aucun doute, être étendue aux terminaux points de vente où un acteur supplémentaire intervient, le commerçant (voir analyse infra) et dans une moindre mesure aux opérations de banque à domicile (home banking). Dans ce dernier cas, en effet, il doit être tenu compte d'un double phénomène : le client a la maîtrise des lieux où est installé le terminal, il a un contractant supplémentaire en la personne d'une entreprise ou d'une administration publique de télécommunications dont l'organisme bancaire, fournisseur de services, n'a pas la maîtrise.

On peut distinguer deux hypothèses de débits illicites : i) débit de compte lié par un tiers non-autorisé : cette hypothèse vise l'utilisation abusive des moyens d'accès du client ou de son mandataire, ce qui suppose la perte ou le vol de ces moyens d'accès, soit la perte de la carte d'accès seule, soit la perte du code seul, soit hypothèse plus dangereuse, perte de la carte et du code d'accès ; ii) la seconde hypothèse est celle de débits illicites par le titulaire de la carte qui, par exemple, prélève davantage que l'avoir disponible sur le compte à vue lié. On distinguera de ces deux hypothèses le cas d'opérations non illicites où le client constate après coup qu'il a été débité d'un montant plus élevé que celui qu'il prétend avoir prélevé. Il n'est pas ici question de comportement illicite ni de la part du

client, ni de la part de la banque, le problème étant essentiellement un problème de preuve du montant de l'opération éffectuée. (v. infra)

3.2. Les solutions contractuelles tendant à la prévention ou à la limitation du dommage

De façon générale, les contrats passés entre la banque et le client donnant à ce dernier les moyens d'accès aux mouvements électroniques de fonds insistent sur l'obligation de vigilance qui lui incombe et non sur l'obligation corollaire de l'organisme financier. Il est certain cependant que des "fuites" peuvent avoir lieu au sein du personnel de la banque. La prévention de ces indiscrétions ne peut trouver une solution adéquate que dans une sensibilisation au respect des règles déontologiques renforcées par des dispositions contractuelles ou réglementaires strictes imposées par l'organisme bancaire employeur.

Trois types de mesures se retrouvent dans les contrats passés entre la banque et le client visant à prévenir ou à limiter l'extension des dommages causés par des débits illicites : i) la confidentialité est requise du client qui ne peut révéler à des tiers le code d'accès aux transferts électroniques de fonds et doit prendre toutes les mesures nécessaires pour éviter la perte conjointe du code et de la carte ;
ii) une obligation de notification est imposée au client en cas de perte de la carte d'accès aux transferts électroniques de fonds. Cette notification est considérée comme essentielle dans la réglementation américaine notamment pour départager les responsabilités respectives de la banque et du client en cas de débits illicites. La forme que revêt la notification est importante ; dans l'intérêt tant de la banque que du client, il s'agit d'assortir la procédure de déclaration d'un certain formalisme tel que, par exemple, l'envoi par le client d'une lettre recommandée avec accusé de réception. Afin de déterminer précisément le moment de la déclaration (car des retraits illicites peuvent toujours avoir lieu le jour même de la perte de la carte ou du code) il faudrait que soient précisées l'heure et même la minute de la déclaration sur l'accusé de réception ;
iii) la consultation des extraits de compte par le client : bien qu'à notre connaissance, l'obligation ne soit imposée ni légalement ni contractuellement au client de consulter régulièrement ses extraits de compte, il est certain qu'une consultation fréquente peut limiter l'extension d'une fraude ; l'envoi d'une documentation périodique par la

banque au client est dès lors requis. La pratique bancaire belge s'est spontanément orientée dans ce sens.

3.3 L'occurrence du dommage : problèmes d'imputation

3.3.1. Les errements de la jurisprudence française

En France, le 1er décembre 1980 (Droit de l'Informatique, 1986/3, p. 124), la Cour de Paris tranchant un litige portant sur l'imputation de débits pratiqués au moyen d'une carte perdue, a dégagé le client de toute responsabilité (la Cour n'évoque pas le fait qu'il y ait eu déclaration ou non; dès lors, la solution vaut donc pour tout retrait qu'il soit antérieur ou postérieur à la déclaration de disparition) au motif que la banque n'avait pas prouvé que le client avait commis une faute dans la garde du code secret et qu'il n'était pas impossible que le système puisse fonctionner sans code. Cette solution, fort à l'avantage du client, mettait la banque dans une situation inconfortable. En effet, il lui était bien difficile de prouver une négligence du client dans la garde du code confidentiel et on voit mal comment elle aurait pu faire face aux fausses déclarations de clients peu scrupuleux continuant d'utiliser la carte. De cet excès, la jurisprudence française est tombée dans un autre excès. Les Cours d'Appel de Pau (17.10.1984, Droit de l'Informatique, 1986/3, 125), de Douai (26.10.1983, Droit de l'Informatique, 1986/3, 121) et de Paris (29.03.1985, Droit de l'Informatique, 1986/3, 122) ont mis à charge du client les retraits frauduleux, même ceux postérieurs à la déclaration de perte de la carte. Les trois cours sont parties du postulat que le système est fiable, qu'il ne peut fonctionner sans le code confidentiel et, de là, ont présumé la négligence du client dans la garde du secret de ce code. Elles ont également estimé que la banque n'avait pas commis de faute en ne prenant pas les mesures d'opposition dès la déclaration de la disparition de la carte au motif que dans les cas d'espèce, le client n'avait pas déclaré la perte ou le vol du code confidentiel. Cette solution est excessive. En effet, comme l'a fait remarquer la Cour de Paris en 1980, il semble que la carte puisse fonctionner sans code. Celui-ci peut encore avoir été formé correctement au hasard ou avoir été aperçu par un tiers lors d'une opération à un terminal, par dessus l'épaule de l'utilisateur. Ces hypothèses sont actuellement considérées comme irréalistes par la jurisprudence française à un point tel d'ailleurs que la Cour de Pau a refusé au client une expertise des systèmes. On remarque qu'il n'est pas

exigé que soit prouvé l'usage du code confidentiel lors des retraits litigieux, usage considéré comme acquis.

3.3.2. La jurisprudence belge

Si la jurisprudence belge s'est orientée dans une direction différente de la jurisprudence française, elle le doit sans doute notamment au contexte contractuel particulier en Belgique, empreint de pragmatisme et aux spécifications techniques des systèmes (on-line).

De façon générale, les contrats passés entre la banque et le titulaire des moyens d'accès reposent sur le système suivant : le titulaire du compte supporte le risque intégral des opérations effectuées à la suite du vol, de la perte ou de l'usage abusif des moyens d'accès, avant d'avoir signalé les opérations illicites ou le risque d'opérations illicites à la banque et que celle-ci ait pu prendre des mesures adéquates pour éviter toute nouvelle opération au moyen de la carte volée ou perdue. La responsabilité du titulaire du compte cesse à partir du moment où il a procédé à la notification à sa banque. Celle-ci doit alors faire diligence et prendre les mesures nécessaires pour éviter la naissance ou l'extension de la perte financière qui pourrait être causée par l'utilisation abusive de la carte.

Ce système est dans les grandes lignes, commun aux trois réglements bancaires relatifs aux cartes de paiement utilisées en Belgique (Mister Cash, Bancontact, Postomat). De façon intéressante, le réglement Mister Cash spécifie très précisément le moment où la banque devient responsable. "La banque garantit qu'aucune opération ne pourra plus être effectuée au moyen de la carte deux heures après que l'agence aura été avisée de la perte ou du vol à condition que cet avis ait été donné dans les heures d'ouverture de l'agence et au plus tard à 15 heures. Si l'avis de perte ou de vol est donné en dehors des heures indiquées au dessus la banque garantit qu'aucune opération ne pourra plus être effectuée deux heures après la prochaine ouverture de l'agence".

Il est important d'avoir ce système à l'esprit pour comprendre et apprécier les décisions rendues respectivement par le Tribunal de Commerce de Liège le 19 janvier 1984 et par la Cour d'Appel de la même ville le 2 février 1985 (2). L'hypothèse était celle de retraits frauduleux à la suite de la perte d'une carte, retraits postérieurs à la déclaration de perte par le

titulaire. La Cour de Liège a estimé que la banque avait une obligation de résultat quant aux mesures d'opposition à prendre suite à la notification de perte de la carte. On notera que les jurisprudences belge et française divergent radicalement pour apprécier la responsabilité de la banque en l'absence de révélation par le client de la perte de son code (outre celle de sa carte). Selon la juridiction belge, si la banque avait pris les mesures d'opposition prévues en cas de perte de la carte, les retraits litigieux n'auraient pas eu lieu, que le client ait ou non divulgué son code secret à une tierce personne.

Un autre affaire (Postomat) a donné lieu à deux jugements, l'un du 23 novembre 1984 rendu par la justice de Paix de Verviers confirmé le 8 janvier 1986 par le tribunal de première instance.
L'affaire concerne la perte de moyens d'accès (une carte Postomat et le code secret repris sur un agenda) en dehors des jours d'ouverture de guichet (le week-end précédant un lundi 1er novembre). Ce n'est que le 2 novembre, à l'ouverture des guichets que le titulaire parvint à prévenir l'office des Chèques Postaux étant donné que la Régie n'avait prévu aucun système de garde la nuit et les jours fériés.
Tant le juge de paix que le tribunal de première instance ont considéré que la Régie avait commis une erreur de conception dans son système affectant la sécurité de façon significative et lui ont imputé la charge des retraits frauduleux.
L'espèce est particulièrement intéressante parce qu'elle pose la question de la responsabilité du fait des services et du niveau de sécurité auquel le consommateur est en droit de s'attendre [2bis].

Quoiqu'il en soit, selon, M. SYX [3], les différents réglements bancaires belges répartissant la responsabilité entre la banque et l'utilisateur reposent sur la notion de faute. D'une part, avant qu'il ait été signalé, l'abus ne peut être dû qu'à une omission ou négligence du titulaire de la carte. D'autre part, après qu'il ait été signalé et que s'est écoulé le temps raisonnablement nécessaire pour intervenir, c'est la négligence de la banque ou de la société de services qui ne prend pas à temps et efficacement les mesures de sécurité qui causent l'abus ultérieur.

Force est cependant de reconnaître que le fondement sous-jacent à cette répartition des responsabilités se rapproche fort d'une théorie des risques, chacune des parties supportant la charge des dommages qu'elle est la plus

apte, à prévenir, au vu du contrôle qu'elle exerce sur les moyens de paiement et sur leur utilisation. Pour pragmatique qu'il soit, ce système aboutit à faire supporter par le consommateur une partie des risques afférents à un système de paiement mis en place par les institutions financières. Certaine doctrine [3bis] prône le principe d'une responsabilité sans faute des institutions financières pour l'organisation et la rationalisation des services bancaires. D'aucuns se sont même demandé s'il n'y aurait pas lieu d'étendre aux services télématiques la récente directive européenne du 25 juillet 1985 relative à la responsabilité du fait des produits défectueux. La question est posée ; sans prétendre la trancher dans cette étude de portée limitée, soulignons qu'une réponse correcte devra évaluer dans quelle mesure les services peuvent être assimilés aux produits pour la définition de la responsabilité.

"Professionnel, écrit M. VASSEUR, le banquier répond de sa technique, il en répond, c'est-à-dire qu'il en est responsable, il en assume le risque, ... [3 ter]. On ne doit pas se cacher que les conséquences pratiques du principe sont lourdes pour l'institution financière prestataire de services sur le plan probatoire particulièrement.
Lorsqu'un usager prétend avoir été victime d'un incident se traduisant par exemple par un débit injustifié, la charge de l'incident pèse sur la banque.
Il lui appartient d'établir que "le système a été construit avec les soucis usuels de prudence et de fiabilité et qu'il fonctionnait dans les conditions normales au moment de l'incident prétendu [3 quater].
Concrètement, nombre d'incidents peuvent empêcher un système de transfert électronique de fonds de fonctionner correctement. Une panne peut l'affecter ; un fraudeur peut en se branchant sur le système, parvenir à faire débiter le compte d'un client, une erreur peut se commettre sans que l'on sache d'où elle émane et à qui elle est imputable.
En vertu de la théorie des risques une présomption pèse sur la banque. Elle ne peut la renverser que si elle prouve la fiabilité du système ou le fait d'un tiers. Logiquement, la banque devrait aussi supporter les conséquences de la force majeure.
Par ailleurs, si le client demeure responsable de sa fraude ou d'une négligence fautive (par exemple divulgation du confidentiel) la preuve de ce comportement incombe cependant à la banque.

3.3.3. Solutions législatives

3.3.3.1. L'approche américaine

-Introduction

La loi américaine a préféré une approche en termes de risques à répartir entre la banque et le client aux raisonnements fondés sur la faute c'est-à-dire sur des critères abstraits qui font supporter au client une part plus ou moins importante du dommage en fonction de la gravité de son manquement [4].

Cette dernière approche entraîne inévitablement un grand nombre de contestations liées à la preuve de la gravité du manquement et se retourne contre l'utilisateur dans la mesure où le tribunal tend à inférer la négligence du client de la seule perte de la carte

-Répartition des risques et plafonnement

La construction américaine consiste en une allocation a priori des risques dans le temps : les débits antérieurs à la déclaration du vol, de l'emploi abusif ou de la perte de ses moyens d'accès sont à charge du client et les débits postérieurs incombent à l'organisme financier. Cette construction qui, en définitive se rapproche fort du système mis au point par les banques belges, en diffère cependant par l'instauration d'une responsabilité plafonnée et progressive en fonction de la rapidité du client à informer l'organisme financier de la perte ou du vol de ses moyens d'accès ou encore de l'irrégularité constatée à la lecture de la documentation qui lui a été remise.

Un plafond général de 50 dollars constitue la règle si dans les deux jours bancaires ouvrables suivant la constatation du vol, de l'emploi abusif ou de la perte de ses moyens d'accès, le client avise son organisme financier. Un plafond plus elevé de 500 dollars ou la disparition du plafond sont des exceptions qui supposent une négligence du client.

- La procédure de déclaration et de rectification d'erreur

Le plafond disparait quand le client n'a pas signalé à sa banque l'emploi

abusif 60 jours à dater de la réception d'un extrait de compte périodique.
Ce délai de 60 jours est extrèmement important à respecter en pratique car à l'expiration de celui-ci, le client est déchu du bénéfice de la procédure de rectification d'erreurs (error resolution procedure). L'erreur est définie de façon extrèmement large et englobe les transferts non autorisés, les transferts incorrects, une erreur informatique ou comptable, une omission sur l'extrait de compte.
La notification du client doit comprendre son identité, son numéro de compte, le montant contesté et ses motifs de croire à une erreur. L'organisme financier doit communiquer ses observations au client dans les 10 jours ouvrables ou à défaut dans les 45 jours de la notification, à la condition de créditer le compte du client du montant litigieux dans les 10 jours.
Si les parties ne parviennent pas à se mettre d'accord dans cette phase de conciliation "préjudiciaire", c'est à la banque qu'il appartiendra de faire la preuve qu'il n'y a pas eu d'erreur.

-Considérations critiques

1) Le législateur américain définit largement le concept d'erreur. Ceci est heureux car, ainsi qu'on l'a signalé, nombre d'incidents peuvent empêcher un système de transferts électroniques de fonctionner correctement. Une panne peut l'affecter, une fraude ou une erreur peuvent se commettre sans que l'on sache d'où elle émane et à qui elle est imputable.
2) Le renversement de la charge de la preuve au détriment de la banque prévu par la loi américaine (§ 909b)) est intéressant à un double titre : il confirme que l'organisation de la preuve réagit sur le fond du droit ; il s'inscrit aussi dans un courant d'opinion tendant à faire reposer sur les organismes financiers le risque des systèmes informatisés mis à la disposition du public.
La solution du renversement n'est cependant pas une panacée en pratique car la banque, maîtrisant les installations techniques, maîtrise aussi les éléments produits par ceux-ci (p. ex des enregistrements informatiques) susceptibles de servir de preuve (v. infra). Cette maîtrise constitue un facteur de risque étant donné le caractère unilatéral des modes de preuve. Par ailleurs, nous réconcilions difficilement le principe du renversement de la charge de la preuve avec la disposition contenue au § 906 f) de l'EFTA suivant lequel la documentation remise au consommateur constitue une "prima facie proof" de l'exécution du transfert.

3) On aura remarqué l'importance dans le système américain de la notification qui conditionne la répartition des risques entre la banque et le client. Dans l'intérêt de celui-ci, un certain formalisme rendant incontestable le fait et le moment de la notification est à recommander (voir nos considérations supra).

4) Primordiale aussi parce qu'elle doit permettre la constatation d'éventuelles irrégularités et que s'y attache une force probante particulière (v. infra), la documentation sur les transferts que doit remettre la banque à son client en vertu de la législation américaine est extrêmement complète, reprenant le montant et la date de l'opération, le type de transfert, l'identification du tiers visé par l'opération.
Cette obligation de la banque participe d'ailleurs d'une <u>obligation très large d'information</u> imposée aux banques américaines en vertu de laquelle elles doivent révéler au client les termes et conditions de l'utilisation du service, lui indiquer ses droits et responsabilités et le prévenir de toute modification dans l'utilisation du service.
La bonne exécution de cette obligation est importante pour que le consommateur puisse utiliser le système en connaissance de cause. Elle s'inscrit d'ailleurs dans le droit fil du devoir de renseignements que les jurisprudence belge et française mettent à charge du professionnel vendeur ou concepteur de systèmes informatiques confronté au profane.

5) Si le délai de 60 jours pour la rectification d'erreurs prend cours à dater de la réception de l'extrait de compte, le délai servant à apprécier la responsabilité du client, dans le cas de vol ou de perte de moyens d'accès, est calculé à partir de la découverte effective par le consommateur de la perte ou du vol.
Ceci risque de poser des problèmes de preuve insurmontables que ne connaît pas le système belge prenant pour critère le moment de la notification [5].
6) Le système américain semble fondé sur le concept de risques mais la notion de faute n'en est pas pour autant écartée puisque la détermination du montant à charge du client dépend de sa diligence à avertir la banque, tout le problème étant d'ailleurs de fixer des plafonds suffisamment élevés pour inciter le client à la prudence.

On assiste en réalité à un glissement, le concept de faute étant

pratiquement évacué pour apprécier le comportement du client dans la garde de ses moyens d'accès mais réapparaissant, par le biais de limites forfaitaires plus ou moins élevées, pour apprécier son comportement une fois que la garde de ces moyens est prise en défaut.

7) La procédure de rectification d'erreurs pourrait servir de référence et être insérée, moyennant adaptations, dans des réglements bancaires (c'est-à-dire en définitive dans des contrats) ou dans une législation spécifique (à supposer que celle-ci soit opportune).
Cette procédure a l'avantage de pourvoir à la rectification dans un délai assez rapide et à l'amiable sans la lourdeur d'une procédure judiciaire [6].
Cette procédure devrait cependant être gérée par un organisme indépendant des banques, suivant l'exemple danois (v. infra).

3.3.3.2. L'approche danoise

a) L'article 21 (5) de la loi danoise de 1984 (en vigueur au 1er janvier 1985) sur le paiement par cartes dispose "... the card issuer shall be liable for payments made after he has been given notice that the card has disappeared or is in the possession of an unauthorised person". Elle s'apparente donc aux systèmes belges et américains décrits ci-dessus. Contrairement au système belge, elle ne fait pas peser en toute hypothèse sur l'utilisateur la charge des risques antérieurement à la déclaration. En effet, l'article 21 1° précise que le titulaire de la carte n'est responsable (à concurrence d'un montant plafonné déterminé par le Ministre de l'industrie) des dommages dus à un usage non autorisé de la carte qu'en cas de négligence lourde - ou lorsque le titulaire tarde à notifier la perte ou le vol de la carte lorsqu'il en a eu connaissance - L'article 21(4) prévoit une responsabilité résiduaire de l'émetteur de la carte. Le système danois nous fait retomber, semble-t-il, dans des difficultés liées à la preuve de la gravité de la faute du consommateur cette preuve devant être rapportée par l'institution émettrice des moyens d'accès (article 22.4).

b) L'ombudsman trouve également sa place dans la récente législation sur les cartes de paiement. Ses pouvoirs sont largement définis et se caractérisent notamment par une possibilité d'action préventive (article 10(2)) notamment quant à la sécurité du système. Il dispose également d'un pouvoir d'injonction si il n'a pas pu faire accepter ses recommandations par voie négociée (article 10 (3)).

4. Le terminal point de vente et la banque à domicile : questions de responsabilité particulières

4.1. Le terminal point de vente

- Les opérations effectuées aux terminaux point de vente mettent en présence un troisième acteur, le commerçant.

Dans les systèmes on-line, les possibilités de faute du commerçant sont peu nombreuses. On songe au mauvais entretien du terminal (encore que celui-ci soit en principe entretenu par la banque) ou à une défectuosité qui abîmerait la carte. En tant que gardien de la machine, il assumerait les dommages provoqués par celle-ci.

Dans les systèmes off-line et les systèmes à confirmation par signature, les possibilités de faute sont plus nombreuses. Outre les hypothèses évoquées dans le paragraphe précédent, la responsabilité du commerçant peut être engagée pour des négligences dans certaines procédures de sécurité telle par exemple la vérification de la conformité de la signature du client avec celle de la carte et la vérification des listes d'opposition.

- Dans certains ordres juridiques, français et belge notamment, la qualification des relations entre l'organisme financier et le client détermine les recours de celui-ci.

A cet égard, l'assimilation des transferts électroniques de fonds à la figure du virement - électronique - n'est pas neutre du point de vue du consommateur surtout si l'on considère l'ordre de virement comme un mandat. Cette qualification, qui n'est défendable que si le paiement est un acte juridique est favorable au consommateur mandant qui se voit, sur base de l'article 1994 et dans les conditions prévues par celui-ci, octroyer une action directe contre la personne que le banquier s'est substituée, ce qui est fréquent dans le cas de transferts internationaux de fonds.

Par contre, la qualification de louage d'ouvrage appliquée à la convention passée entre le consommateur et sa banque ne lui est pas favorable sur le plan pratique car, par le jeu de la relativité des conventions posé (article 1165 du Code civil), il se voit privé de tout recours contractuel direct

contre la banque correspondante. Et les recours de type délictuel fondés sur l'article 1382 du Code civil sont aléatoires.

De façon générale, étant donné la multiplicité des parties à une opération de transferts de fonds (banque du donneur d'ordre, banque intermédiaire, banque du bénéficiaire, réseaux de transmission, propriétaire du terminal,...) et les difficultés de la localisation de la cause d'un dommage, on prônera, au moins de lege ferenda, la responsabilité, pour l'ensemble de l'opération, de l'émetteur des moyens d'accès au transfert électronique. A condition bien sûr que le consommateur se soit conformé aux précautions contractuellement ou légalement définies qui gouvernent l'utilisation des moyens d'accès.

4.2. La banque à domicile (Home Banking)

La banque à domicile soulève des problèmes de responsabilité différents de ceux que soulèvent les D.A.B. et les T.P.V. Le transport de l'information se fait, dans la plupart des pays européens sur des réseaux de télécommunications publics jouissant d'un monopole et d'une limitation légale de responsabilité. Ces réseaux n'offrent pas toujours une très grande sécurité quant au transport correct du message (pas d'encryptage effectué par l'intégrateur ou le transporteur) et du point de vue de l'accès. Aussi la banque à domicile n'est-elle pas encore très développée bien que des procédures de sécurité soient prévues (code confidentiel, numéros de transaction, listes arrêtées par le donneur d'ordre de numéros de compte habilités à percevoir des fonds).
Contrairement aux D.A.B. et aux T.P.V. où la banque ou le groupement interbancaire gérant le système est le répondant unique du client (installation des terminaux, location des lignes, accords avec l'administration ou l'entreprise de télécommunications) le client, est ici un abonné de l'administration des télécommunications ou de l'intégrateur privé.; il s'équipe lui-même des appareils nécessaires et est usager des services fournis par l'administration ou l'intégrateur privé. Le fournisseur du service n'est, comme le client, qu'un simple usager du service de télécommunications.

Dès lors, une présomption de responsabilité de la banque ne se justifierait plus ici vu qu'elle n'est pas maître de sa technique. Le rôle de l'intégrateur est en effet déterminant. Ainsi se comprend la clause 9 du contrat-type

allemand qui met à charge du client tous les dommages résultant d'une application incorrecte ou frauduleuse de son PIN et de son TAN (numéro de transaction) tandis que la banque n'est responsable des fautes qui lui sont imputables que dans la mesure où elles ont participé à la naissance du dommage.

Il reste qu'une telle clause opère un transfert de responsabilité sur le client, lequel n'a pas davantage la maîtrise de la technique utilisée et se heurtera aux problèmes de preuve que l'on connaît ; elle n'est donc pas plus justifiée
De plus, les incidents résultant de fraudes de tiers durant le transfert du message restent à charge de l'utilisateur. Celui-ci est présumé avoir été négligent dans la garde de son PIN et/ou TAN. S'il parvenait à démontrer le contraire, une faute de l'intégrateur ou du transporteur par exemple, son sort ne serait pas plus avantageux, vu que cet acteur bénéficie d'une limitation de responsabilité.

Ces remarques plaident pour deux types de mesures :

1. des mesures techniques et d'auto-discipline tendant à améliorer la sécurité des systèmes;

2. des mesures légales visant à améliorer le sort de l'usager des services de télécommunication fournis par l'intégrateur et le transporteur.

Le home banking présente une particularité par rapport aux systèmes DAB-TPV : l'intervention d'un tiers neutre en regard de la relation entre la banque et le client. Les problèmes de preuve pourraient s'en trouver singulièrement simplifiés si un acteur "au-dessus de tout soupçon", l'intégrateur-transporteur, en l'occurrence, conservait un certain nombre d'informations à des fins probatoires.

5. Conclusions - Pistes de réflexion

5.1. Au plan juridique

1) De ce panorama des problèmes de responsabilité suscités par les transferts électroniques de fonds et des solutions contractuelles ou légales appelées à les régler, on retiendra qu'une approche en termes de

"risque" telles que l'approche américaine et l'approche des banques belges, encore que pondérée sur certains points par l'exigence d'une faute, est plus adéquate qu'un système fondé sur des critères abstraits imputant le dommage totalement ou partiellement en fonction de la gravité de la faute.

ii) Pivot de ce système, la documentation remise par la banque au client se doit d'être complète, à jour et fréquente. Celui-ci se voit "obligé" [7] de la consulter attentivement afin de pouvoir procéder, le cas échéant, à la notification sous une forme qui ne souffre pas contestation, cette notification ayant pour effet, au regard de la jurisprudence belge du moins, de couper le lien de causalité entre le comportement antérieur du client même fautif et les retraits ultérieurs.
Documentation d'une part, notification d'autre part ne sont que deux versants de l'obligation d'information entre parties dont le banquier en tant que professionnel assume la plus grande part. C'est la même obligation d'information qui lui impose d'ailleurs de communiquer au client le texte de ses conditions générales et leur changement éventuel en cours de contrat.

iii) La procédure américaine de rectification, quoique complexe dans ses modalités, constitue une tentative intéressante dans son principe car elle vise au réglement rapide et équitable des "erreurs" éventuelles.
Très favorable au consommateur, la législation américaine prévoit même que la banque effectuera un crédit provisoire du compte du client correspondant au montant de l'erreur alléguée si elle ne peut lui répondre dans les 10 jours ouvrables à dater de la notification. Ceci nous met aux antipodes de la pratique apparemment répandue dans les milieux bancaires américains d'imputer automatiquement les débits illicites sur les comptes du client non liés aux transferts électroniques de fonds (ex. comptes d'épargne....).

iv) A qui adresser sa demande en rectification quand le réseau de distributeurs est un réseau partagé entre plusieurs institutions financières. On peut très bien concevoir qu'une erreur surgisse suite à une opération initiée sur un terminal d'une banque A à partir de moyens d'accès délivrés par une banque B.
Le principe devrait être à notre avis que le consommateur a toujours le droit de s'adresser à l'institution émettrice des moyens d'accès, quitte pour cette dernière à procéder à un réglement ultérieur avec l'institution

gérant et/ou possédant le terminal.
v) L'idée d'un ombudsman appelé à traiter les différends entre le consommateur et la banque est intéressante mais difficile à mettre en oeuvre au niveau européen.

5.2. Au plan technique

D'entrée de jeu, on se doit de signaler que la séparation des plans technique et juridique est faite pour des raisons d'ordre dans l'exposition mais que les liens unissant les deux plans sont nombreux.

1. Les progrès techniques dans l'évolution technique vont préciser par touches successives le véritable rôle du droit, sans doute réduire les risques de dommages et avoir une incidence sur la fréquence et la gravité des hypothèses de responsabilité.

2. Le niveau technique de sécurité atteint par le secteur bancaire peut servir de référence pour apprécier la responsabilité d'une banque offrant au consommateur un service obsolète et peu sûr au regard du niveau technologique du moment. Une codification des normes de sécurité par le secteur lui-même , quoique rendue problématique par la rapidité de l'évaluation technologique, pourrait rendre l'appréciation plus aisée.

3. Parmi les solutions techniques concrètes pouvant diminuer les risques d'occurrence des dommages, on en épinglera trois.

a) On pourrait imaginer que chaque distributeur de billet offre au consommateur une possibilité de mise en opposition des moyens d'accès pour éviter l'usage abusif de ceux-ci et lui délivre un reçu comportant le moment exact de l'opposition.

b) Il a été également suggéré de munir les distributeurs de billets de caméras qui permettraient d'identifier la personne initiant la transaction et au moins de vérifier si c'est le titulaire des moyens d'accès qui a ou non procédé au transfert. L'objection majeure à l'encontre de cette suggestion est l'atteinte aux droits de la personnalité, droit à l'image et vie privée notamment, que sa mise en oeuvre risque d'entraîner.

c) D'autres techniques, plus sophistiquées que le code secret sont

actuellement à l'étude : telles que la reconnaissance à distance d'une caractéristique physique de l'individu (par exemple la voix ou les empreintes digitales) ou la reconnaissance dynamique de la signature. Toutes ces techniques visent à augmenter la probabilité que l'utilisateur des moyens d'accès soit bien le titulaire ou l'attributaire légitime de ceux-ci en permettant de rapporter le message à une personne physique déterminée.
Le problème fondamental en droit sera de déterminer la valeur juridique de ce mode d'identification (v. infra).

LE TRANSFERT ELECTRONIQUE DE FONDS DANS SES APPLICATIONS "GRAND PUBLIC" : PROBLEMES JURIDIQUES GENERAUX

(Document de travail)

Marc Schauss
Xavier Thunis

Assistants au Centre de
Recherches Informatique
et Droit (C.R.I.D.)
Rempart de la Vierge, 5
5000 NAMUR

Juillet 1987

Notes du point V

[1] Pour plus de détails voir E. SHINN, An Overview of Unauthorized Electronic Fund Transfers : Alternatives in Reducing Consumer Liability Commercial Law Journal, 1985, p. 220.

[2] Sur ces décisions et pour un commentaire, voir J.P. BUYLE, La carte de Banque à Pistes Magnétiques, Rev. dr. Comm. belge, 1984, p. 658 et s ; B. AMORY et X. THUNIS, note sous Trib Comm. Liège 19 janvier 1984, Droit de l'Informatique, 1984, n° 2, p. 29 ; B. AMORY note sous Appel Liège 22 février 1985 Droit de l'Informatique, 1985, n° 3, p. 28 ; Voir aussi l'intéressante enquête LOSING AT CARDS, An investigation into consumer's Council 1985. Cette enquête donne pour le Royaume-Uni un aperçu des hypothèses survenant en pratique.

[2bis] Pour plus de détails voir L. SIMONT et A. BRUYNEEL, chr. citée p. 53 et s.

[3] D. SYX, op. cit., p. 32

[3bis] voir notamment N. LHEUREUX, Le transfert électronique de fonds au regard du contrat bancaire, la Revue du barreau canadien, 1985, p. 177 et s; sur les services télématiques en général, Y. POULLET, Liberté des flux de données et Droit communautaire, CELIM, 2-3 avril 1987, p. 55 et s.

[3 tris] M. VASSEUR, Aspects juridiques des nouveaux moyens de paiement, Revue de la Banque, 1982, p. 592 et s.

[3 quater] P. LECLERCQ, Les problèmes juridiques posés par les nouveaux moyens de paiement, Droit et économie, ANDD n° 42.

[4] D. SYX, op. cit., P. 104 et s.

[5] Pour plus de détails, M. ELLIS et F. GREGURAS, The Electronic Fund Transfer Act and the Federal Reserve Board Regulation E. A compliance Guide for Financial Institution, Prentice Hall New Jersey, 1983, p. 144

[6] Comparer les propositions faites dans CNC, Rapport du groupe de travail sur les aspects juridiques des nouveaux moyens de paiement, p. 84 et s.

[7] Sur l'obligation du client de consulter ses relevés et extraits de compte voir notamment J. VEZIAN, La responsabilité du banquier, LITEC, 1983, p. 51 et s.

VI LE TRANSFERT ELECTRONIQUE DE FONDS - QUESTIONS DE PREUVE

1. Introduction

On a déjà indiqué que les opérations financières illicites amènent inévitablement la réflexion à se porter sur des questions de preuve, détermination de la charge de la preuve et des éléments probatoires admissibles.

Il peut y avoir en outre des cas où, bien que l'accès soit licite, un désaccord existe entre le client et sa banque par exemple sur le montant retiré ou transféré au distributeur automatique de billets ou au terminal point de vente.

Supposons par exemple un client qui a donné des instructions au terminal pour retirer 5000 FB et qui n'en reçoit que 4000 (ou, cas plus favorable, qui en reçoit 6000).

Opération inverse (ne constituant d'ailleurs pas un transfert électronique), un client dépose au terminal une somme de 5000 FB et la banque n'enregistre qu'un dépôt de 4000 (ou cas plus favorable enregistre un dépôt de 6000 FB). Quels sont concrètement les élements dont disposent le client et la banque pour établir leurs prétentions, ces éléments se voient-ils reconnaître une valeur en droit ? Dans quels cas la charge de la preuve incombe-t-elle au client, dans quel cas incombe-t-elle à la banque? L'analyse se fait au départ des droits belge et français.

2. Les supports d'information dans le transfert électronique de fonds

Les principes régissant le droit de la preuve accordent la prééminence à l'écrit signé. Aussi examinons nous ici les supports d'information papier [1] qu'engendre le transfert électronique de fonds, supports susceptibles le cas échéant de se voir reconnaître une force probante particulière en droit :

1) L'enregistrement par écrit, sur "bandes journal" (logging) dans le

distributeur automatique ou le terminal point de vente de toutes les opérations se rapportant au terminal en question.

ii) Les tickets remis au client par le terminal et lui fournissant un résumé de l'enregistrement de l'opération en question.

iii) On ajoutera à ces documents les extraits de compte délivrés par les banques pour constater l'opération financière d'un client, qu'elle s'effectue par voie électronique ou non.

3. Force probante de ces supports-papier - Principes

La preuve peut avoir pour objet de déterminer soit l'identité de l'auteur de l'acte (est-ce ou non le titulaire des moyens d'accès ?) soit la réalité de l'opération ou son contenu [2].

Si l'avantage de la télématique est la rapidité accrue dans la conclusion de contrat, son inconvénient est la fugacité. Les mentions apparaissent et disparaissent à l'écran rendant problématique la constitution d'une trace de ce qui est échangé.

Par ailleurs, même si l'on parvient à établir l'existence et le contenu du contrat, l'identité des parties à ce contrat n'est pas certaine pour autant. L'identification du terminal ne permet pas de "remonter" à l'identité de la personne qui opère la transaction. Même un mot de passe ou un code secret n'identifient que l'abonné au réseau mais pas la personne qui effectue l'opération.

3.1 le principe : la prééminence de la preuve écrite

L'article 1341 du Code civil, texte de portée générale, constitue une pièce essentielle du régime probatoire : "Il doit être passé acte devant notaire ou sous signature privée de toutes choses excédent la somme ou valeur de trois mille francs, même pour dépôt volontaires ; et il n'est reçu aucune preuve contre et outre le contenu aux actes. Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce".

L'application de ce principe aux transferts électroniques de fonds amène à s'interroger sur la valeur probante des supports-papier décrits plus haut

d'autant plus que la signature écrite, expression de la personnalité d'un individu et de son adhésion au contenu d'un acte, disparaît.

Des débats parfois animés ont eu lieu pour savoir si l'introduction d'un code secret, ou de façon plus subtile l'utilisation d'un code secret dans le cadre plus large de la procédure d'accès strictement déterminée doit être ou non considérée comme une signature de type électronique. M. SYX (3) a toujours vigoureusement plaidé pour une conception "non dogmatique" de la signature et considère que la différence entre une signature électronique et une signature manuscrite est plus formelle que fondamentale, l'essentiel étant que l'on puisse induire de l'utilisation de signes manuscrits ou électroniques l'appropriation d'un acte par le client.

Ses contradicteurs font observer que le code secret, contrairement à la signature manuscrite, n'est pas lié à la personne et ne la caractérise donc pas. Par ailleurs, intervenant au début des opérations pour ouvrir l'accès au système de transfert, elle ne saurait, comme la signature apposée au bas d'un acte, authentifier le contenu de celui-ci.

Notons que les recherches en cours sur les signatures électroniques liées à une caractéristique physique de la personne, si elles aboutissent, permettront d'identifier l'auteur de l'opération.

3.2. Tempéraments

Les considérations émises ci-dessus impliquent elles que, pour l'instant, les transferts électroniques de fonds, ne donnant lieu à aucune trace écrite signée sont refoulés dans les "ténèbres préjuridiques" ? Cette conclusion trop rapide doit être nuancée :

3.2.1 Le droit civil distingue nettement la preuve des actes juridiques de celle des faits juridiques, seuls les premiers étant soumis au prescrit de l'article 1341 du Code civil.
La conséquence en ce qui concerne le régime de la preuve est importante : le fait juridique peut être prouvé par tous moyens de droit, présomptions, témoignages, aveu ...

La majorité des auteurs n'a pas, à notre avis, assez réfléchi à la nature des opérations de transferts électroniques de fonds en semblant considérer

automatiquement qu'il s'agit d'actes juridiques. Cette conception devrait à tout le moins être nuancée si l'on tient compte que la modalité électronique du transfert est une simple exécution par le banquier de l'obligation contractée sur base d'un contrat de services accessoire à un dépôt ou à une ouverture de crédit [3bis].

3.2.2. Les exceptions légales à la prééminence de l'écrit

1. Les transactions relatives à de petits montants (jusque 5000 FF en France, jusque 3000 FB en Belgique) peuvent être prouvées par tout moyen de droit .

2. L'article 1341 du Code civil s'applique quand la matière, c'est-à-dire l'acte, relève du droit civil (art. 1341 al. 2). En matière commerciale, la preuve est libre et tous les modes de preuve sont recevables sous le contrôle du juge.

Lorsque le contrat est conclu par un particulier, l'acte passé sera un acte mixte, c'est-à-dire commercial dans le chef du serveur et civil dans le chef de l'utilisateur.

Quand l'acte est mixte, l'article 1341 réserve ses rigueurs au commerçant qui peut éprouver des difficultés à produire une preuve écrite signée de l'acte juridique passé sur le réseau.

3. L'article 1341 ne s'applique pas davantage lorsqu'il n'a pas été possible à celui qui invoque le fait de se procurer une preuve littérale de l'obligation qui a été contractée envers lui (Code civil art. 1348), ou lorsqu'il existe un commencement de preuve par écrit (Code civil, art. 1347).

Il semble que l'utilisation de systèmes informatiques ou de réseaux télématiques, du moins dans les applications grand-public, constitue l'exception prévue à l'article 1348 du Code civil. Cette interprétation s'accorde, en tous cas, avec la conception extensive, en jurisprudence, de l'impossibilité de se réserver une preuve écrite.

3.2.3. La force obligatoire de l'article 1341 du Code civil

Selon de nombreux auteurs, l'article 1341 du Code civil n'est ni une disposition impérative, ni une disposition d'ordre public. Ainsi, il serait possible de déroger à la règle de l'écrit dans une convention relative à la preuve précisant que les opérations juridiques passées sur le réseau peuvent être prouvées par toutes voies de droit.

Conclusion : Le principe de la prévalence de l'écrit connaît de nombreuses exceptions et atténuations. Les conventions passées entre le client et la banque comportent d'ailleurs des dispositions relatives à la preuve et à la signature. Ainsi l'article 6 du règlement Bancontact indique : "Preuve des transferts électroniques de fonds : Toutes les données importantes aux opérations effectuées dans ce système sont enregistrées. Pour certaines opérations le porteur de la carte reçoit une documentation sous la forme de tickets.
Les documents (tickets) délivrés par le guichet ou par le terminal point de vente ne constituent pas une preuve de l' (des) opération (s) qu'ils mentionnent mais sont seulement fournis au porteur de la carte à titre d'information ou pour lui permettre un contrôle.

Le porteur de la carte et/ou le titulaire du compte et l'organisme financier acceptent, chacun pour ce qui les concerne, que la bande-journal ou un support d'information équivalent, sur lesquels sont enregistrés les données relatives à toutes les opérations à chaque guichet automatique ou chaque terminal terminal point de vente, constitue un procédé de preuve par écrit contraignant et suffisant."

De même, l'article 3 §3 du règlement Mister Cash indique que "... le fait pour le client d'introduire sa carte et son code personnel dans l'appareil équivaut à la signature d'un ordre de virement en faveur du commerçant ou service public chez qui l'appareil est installé ...".
De telles conventions, sont sévères pour les titulaires de cartes dans la mesure où se trouve consacrée contractuellement la valeur probante de "documents unilatéraux", en l'occurrence d'enregistrements informatiques dont le client n'a pas la maîtrise [3tris].

A notre avis, l'enregistrement informatique pourrait constituer au plus un élément de preuve parmi d'autres dont le juge pourra induire une

présomption de fait (Code civil article 1349).

A titre de mesure minimale, l'enregistrement informatique devrait faire l'objet d'un examen par un expert indépendant de la banque. Les problèmes relatifs à la conservation des enregistrements informatiques devraient aussi être soigneusement réglés. Comme le suggère l'exposé ci-dessus, le problème n'est pas dans cette matière d'échapper à la prééminence de la preuve écrite mais de puiser dans les techniques modernes des éléments ayant une fiabilité et si possible un caractère contradictoire tels qu'on puisse en tirer des présomptions sur l'existence et le contenu d'un acte ainsi que sur l'identité des parties à celui-ci. A cet égard, la carte à mémoire dont l'utilisation se traduit par un dédoublement de l'information qui sera conservée sur la carte elle-même semble faire renaître un caractère contradictoire (à tout le moins doublement unilatéral) qui jusqu'ici fait défaut.

4. Charge de la preuve

Suivant l'article 1315 du Code civil, la charge de la preuve pèse sur celui qui réclame l'exécution d'une obligation. Celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation.

Appliqués aux versements et aux retraits de fonds, ces principes donnent les résultats suivants [4] :

i) dans le cas d'un versement de fonds, le client agit en qualité de dépositaire et donc de créancier ; il doit dès lors prouver l'existence et l'importance des fonds versés.
ii) dans le cas d'un retrait, la banque devrait fournir la preuve du fait et du montant du retrait.
iii) pour les virements électroniques, le client devrait prouver l'ordre (existence et contenu), la banque devant prouver son exécution.

Inutile de préciser que l'application pratique de ces principes est très malaisée si les modes de preuve pertinents n'existent pas (voir considérations supra).
Au-delà de l'énoncé des principes un peu formels et d'ailleurs nuancés par la doctrine moderne qui met l'accent sur la collaboration des parties à la charge de la preuve, il faut, à la suite de l'excellent Rapport du Conseil

National du Crédit [5], souligner à quel point la charge de la preuve réagit sur les droits effectivement reconnus à la banque d'une part, au client d'autre part en cas de vol ou de perte de carte (et plus généralement des moyens d'accès).
S'il appartient au banquier en sa qualité de professionnel, de rapporter la preuve de la fiabilité des systèmes, ceci signifie que le banquier doit supporter les conséquences des incidents inexpliqués ou dus à la force majeure. Ceci signifie aussi qu'à défaut de rapporter positivement la preuve d'une imprudence du client dans la garde de son code, la banque devra assurer la responsabilité de prélèvements frauduleux, ceux-ci pouvant toujours être dus à une défaillance du système ayant fonctionné par exemple sur simple introduction de la seule carte.

Par contre et ceci semble se dégager des plus récentes décisions françaises, dans la mesure où les sytèmes sont supposés fiables, c'est au client qu'il appartiendra de rapporter la preuve qu'il n'a commis aucune faute dans la garde de son code confidentiel.

5. Eléments de droit comparé

Le présent chapitre n'a pas pour objet de présenter une synthèse comparative des différents systèmes de preuve [6] face à l'informatique et à la télématique.

- Signalons simplement en France, la réforme du 12 juillet 1980 qui est notamment venue tempérer l'exigence de la preuve écrite en élargissant le domaine de la liberté de preuve pour des actes juridiques d'un montant inférieur à 5000 FF. Réforme à la fois limitée et importante :
- limitée parce qu'elle ne remet pas en cause la prééminence de la preuve écrite.
- importante parce qu'elle vise le champ en définitive très large des opérations courantes passées entre commerçants et particuliers (entre commerçants la liberté de preuve joue quel que soit le montant).

La question demeure entière cependant de savoir comment organiser la liberté de preuves dans le cadre ainsi tracé [7].

- Comme la loi française, la loi grand-ducale du 22 décembre 1986 prévoit la fixation par règlement du montant au-delà duquel un écrit est requis.

Ce montant est actuellement fixé à 100.000 FB. L'article 1348 nouveau prévoit que le principe de l'écrit reçoit exception ..."lorsque l'une des parties n'a pas eu la possibilité matérielle et morale de se procurer une preuve littérale de l'acte, ..." ou encore "lorsqu'une partie ou le dépositaire n'a pas conservé les titres originaux et présente des reproductions monographiques et enregistrements informatiques effectués à partir de ces originaux sous la responsabilité de la personne qui en a la garde...".

- Une recommandation du Comité des Ministres du Conseil de l'Europe (n° R (81) 20, 11 décembre 1981) vise à l'admissibilité à titre de preuve des documents de nature informatique sous condition de fidélité, d'exhaustivité, de lisibilité et d'ordre dans la conservation.

- Plus directement lié à cette étude, l'Electronic Fund Transfer Act, dont l'objet n'est pas de réformer le droit de la preuve américain, comporte cependant des dispositions importantes relatives à l'aménagement de la charge de la preuve.

1. Le § 905 de l'EFTA impose à l'institution financière de remettre au client une documentation écrite pour chaque opération effectuée au départ d'un terminal et un extrait de compte périodique reprenant les informations sur le compte et les mouvements qui l'affectent. Cette documentation, en vertu du § 906 f) constitue, en cas de procédure judiciaire, une "prima facie proof" que les transferts repris se sont déroulés de la façon indiquée.

2. Le § 909 b de l'EFTA indique que dans toute action impliquant la responsabilité d'un consommateur pour un transfert non autorisé, la charge de la preuve repose sur l'institution financière. Force est de reconnaître, à la lecture, que la rédaction de cet article ne brille pas par sa clarté.

Notes du point VI

[1] L'exposé qui suit s'inspire largement de l'ouvrage déjà cité de D. SYX, p. 57 et s.

[2] l'ex posé qui suit reprend de larges passages de l'étude de Y. POULLET et X. THUNIS, Introduction aux aspects juridiques de la télématique in la Télématique, Story-Scientia, T. I., p. 158 et s. ; pour une étude d'ensemble, voir M. FONTAINE, la preuve des actes juridiques et les techniques nouvelles paru dans "La preuve", 1987, 42 pages ; en ce qui concerne la télématique professionnelle voir B. AMORY et X. THUNIS, Dématérialisation, authentification et responsabilité in Les transactions internationales assistées par ordinateur, LITEC, 1987, p. 71 et s.
l'opération.

[3] D. SYX, Naar nieuwe vormen van het handtekening ? Het probleem van de handtekening in het elektronisch rechtsverkeer, KB 1985.

[3bis] Pour une discussion M. FONTAINE, op. cit., p. 29.

[3tris] Ce type de clause aboutit à décharger la banque de son obligation de vérification de signature, et constitue en fait une exonération de responsabilité dont la validité est discutable. Pour une discussion N. LHEUREUX, Le transfert électronique de fonds en regard du contrat bancaire. La revue du barreau canadien 1985 vol. 65 p. 163 et s.

[4] Voir D. SYX, "Aspects juridiques ..." déjà cité p. 83 ; sur l'hypothèse d'un dépôt dit "trésor de nuit" et de la charge de la preuve cf R.T.D. Comm. 1982, p. 285

[5] Conseil National du Crédit, rapport du groupe de travail sur les aspects juridiques des nouveaux moyens de paiement, juillet 1986, p. 54 et s.

[6] Pour une étude de ce type, voir B. AMORY et Y. POULLET, Le droit de la preuve face à l'informatique et à la télématique : approche de droit comparé, Droit de l'informatique n °5, p. 11 et s.

[7] Pour plus de détails voir notamment J. HUET La protection des biens, les obligations contractuelles, la preuve in Emergence du droit de l'Informatique, Editions des Parques, 1982, p. 47 et s.

VII LE PAIEMENT PAR TRANSFERT ELECTRONIQUE - MOMENT ET REVOCATION - CONFLITS ENTRE ORDRES DE PAIEMENT

1. Moment du paiement [1]

L'enjeu de la question est multiple. En effet, le paiement, une fois définitif, ne peut plus être révoqué. De plus, un conflit peut naître entre différents ordres de transferts successifs, conflit dû à un traitement juridique particulier accordé au transfert de fonds par des techniques particulières (ex. chèques). Ensuite, les transferts effectués au profit d'un bénéficiaire ou d'une banque bénéficiaire tombée en faillite subissent un sort différent suivant que le paiement est définitif ou non au moment de la déclaration de faillite. Enfin, le moment du paiement sert de référence pour déterminer si le destinataire a été mis en possession des fonds dans le délai convenu et pour déterminer si l'institution financière mandatée pour exécuter l'ordre de transfert s'est acquittée de sa tâche ponctuellement.

La Commission des Nations Unies pour le droit du commerce international (CNUDCI) a répertorié les différentes solutions[2]. Il apparaît que le moment où le paiement devient définitif est variable suivant les droits nationaux. Les différents moments pris en considération sont les suivants.

1. Moment du débit du compte du donneur d'ordre
2. Moment du crédit du compte de la banque du bénéficiaire.
3. Moment où la banque du bénéficiaire est avertie du transfert porté à son compte.
4. Moment où la banque du destinataire accepte le transfert porté à son compte.
5. Moment du crédit du compte du bénéficiaire.
6. Moment où le bénéficiaire est averti du transfert à son compte.

Plusieurs constatations méritent d'être faites : d'abord, certains de ces moments posent des problèmes quant à leur détermination ou à leur preuve en cas de transfert électronique. Un décalage entre le moment où l'opération est initiée et celui où le paiement devient définitif présente des avantages et des inconvénients. Les avantages consistent d'une part, dans la possibilité pour la banque de rectifier des erreurs dans l'intervalle

et d'autre part, dans un coût moins élevé du service (du moins, théoriquement) dans la mesure où la banque se rémunère partiellement par la mobilisation des fonds.
Les inconvénients résident dans l'insécurité résultant de la faculté de révocation de l'ordre de paiement, dans le délai de non disposition des fonds. Le paiement électronique jouit d'un avantage difficile à expliquer rationnellement au regard du paiement au comptant ou par chèque, lequel ne souffre en principe pas la révocation de l'ordre de paiement une fois le chèque émis. C'est ce qui a amené la France à légiférer dans le sens de l'irrévocabilité du paiement par carte (article 22 de la loi du 11 juillet 1985). Cette disposition qui en réalité, ne fait que confirmer légalement la pratique contractuelle française, prévoit qu'il ne peut être fait opposition qu'en cas de perte ou de vol de la carte, ou de redressement ou de liquidation judiciaire du bénéficiaire, de sorte qu'en cas d'insatisfaction du consommateur quant au produit qui lui a été fourni ou au service qui lui a été presté, le litige doit se régler a posteriori, ce qui rencontre les intérêts et désirs des bénéficiaires des paiements c'est-à-dire actuellement, des commerçants qui participent au système.
Cette solution, qui rencontre également les voeux des banques ne s'inscrit pas dans la ligne des lois françaises récentes sur le crédit notamment, qui afin de protéger le consommateur contre les effets rigoureux de l'abstraction cambiaire, interdisent l'utilisation des lettres de change ou atténuent la portée de l'inopposabilité des exceptions. (cfr. Art. 17 Loi n° 78-22 du 10 janvier 1978 relative à l'information et à la protection du consommateur dans le domaine de certaines opérations de crédit ; cfr. aussi chapitre I de la loi n° 79-596 du 13 juillet 1979 relative à l'information et à la protection des emprunteurs dans le domaine immobilier).

Les autres pays n'ont pas pris de mesure légale analogue.
En droit belge, la solution générale relative au moment du paiement est celle du moment où le compte du bénéficiaire est crédité.
Quant à la loi danoise de 1984 sur les cartes de paiement, elle ne contient aucune disposition réglant le problème.
Enfin, au point de vue international, des difficultés peuvent surgir en raison de la diversité des solutions. En effet, la banque d'un pays autorisant la révocation de l'ordre de paiement risque, suite à l'ordre de révocation par son client, de ne pas trouver de prolongement à son action auprès de la banque du bénéficiaire appartenant à un Etat consacrant

l'irrévocabilité du paiement électronique.

2. Conflits entre ordres de paiement

Les situations de conflit entre ordres de paiement peuvent survenir entre instruments de paiement de même nature ou de natures différentes. L'hypothèse d'un conflit entre un ordre de paiement électronique et un ordre incorporé dans un effet de commerce (Chèque, lettre de change) est réglée par les conséquences d'une règle valant dans certains pays selon laquelle la propriété de la provision est transférée au bénéficiaire dès l'émission de l'effet de commerce. La conséquence est que le banquier doit donner la préférence au porteur de l'effet. L'hypothèse d'un conflit entre différents ordres de paiement électronique alors que le compte est insuffisamment approvisionné, elle, n'est pas résolue directement.
Il appartient au donneur d'ordre de préciser ses instructions en cas de conflit.

Notes du point VII

1 Sur l'importance de cette question, voir B. AMORY et X. THUNIS, Dématérialisation, authentification et responsabilité in Les transactions internationales assistées par ordinateur, LITEC, 1987, p. 111 et s.

2 Draft Legal Guide on Electronic Fund Transfers, 30 april 1985, A/CN9/266/Add.1.

VIII. ASPECTS PENAUX DES TRANSFERTS ELECTRONIQUES DE FONDS

L'importance des dommages résultant de fraudes informatiques bancaires[1] et la perspective d'un accroissement des fraudes amènent le monde bancaire [2] et certains juristes [3] à se plaindre de lacunes de la loi pénale. Le discours est étonnant : alors que les institutions financières avancent l'argument de la sécurité des systèmes tant pour étendre leurs nouveaux services que pour se défendre dans les procès en responsabilité au point de convaincre les juges de la totale fiabilité de leurs systèmes [4], elles réclament des actions législatives pour venir à leur secours ; logique étrange également chez certains juristes qui revendiquent une révision de la législation pénale en alléguant curieusement que les fraudes informatiques sont importantes et .. malaisées à découvrir [5].
Parmi les Etats membres des C.E., seuls le Danemark [6] et l'Allemagne [7] ont introduit des normes pénales spécifiques à la fraude informatique. Des textes sont à l'état de projet en France [8]. Dans les pays ne connaissant pas de législation pénale spécifique, jurisprudence et doctrine sont divisées sur les qualifications pénales de ces nouveaux comportements.

Les fraudes qui portent sur les transferts électroniques de fonds "grand-public" se réalisent généralement au moyen d'une carte, procédé d'identification le plus couramment utilisé actuellement (1). Dans ce cas, la fraude peut être le fait du titulaire de la carte ou celui d'un porteur illégitime. Des fraudes peuvent également être commises sans l'aide d'une carte (2).
Le raisonnement se fait sur base des droits français et belge.

1. Fraude perpétrée au moyen d'une carte

1.1. L'auteur est le titulaire de la carte.

Le titulaire d'une carte magnétique peut commettre différents types de fraude : il peut outrepasser le solde créditeur de son compte soit en retirant davantage que le disponible, soit en payant un commerçant avec des sommes qu'il n'a pas (1.1.1.). Cette hypothèse n'est en principe possible que dans le cas des systèmes off-line ; il peut aussi utiliser frauduleusement une carte annulée ou périmée (1.1.2) ; des sommes

peuvent avoir été obtenues ou utilisées au moyen d'une carte obtenue frauduleusement (1.1.3) ; enfin, le titulaire de la carte peut en avoir déclaré frauduleusemnt la perte ou le vol tout en continuant de l'utiliser (1.1.4.).

1.1.1. Dépassement du solde créditeur

Cette hypothèse a été abondamment discutée en doctrine et en jurisprudence. La répression est certaine en Allemagne ; l'impunité semble certaine en France et la solution demeure aléatoire en Belgique.

L'Allemagne, depuis la réforme du droit pénal économique, connaît une incrimination spécifique à l'hypothèse [9].

En France, l'incrimination pénale était incertaine [10] jusqu'à l'arrêt de la Cour de Cassation du 24 novembre 1983 qui a très clairement affirmé que l'hypothèse ne rentrait dans le champ d'application d'aucun texte pénal en vigueur [11]. L'hypothèse envisagée par la Cour de Cassation était celle d'un retrait de billets à un distributeur automatique de billets, supérieur à l'avoir en compte. Certains auteurs distinguent cette hypothèse de celle du paiement effectué auprès d'un commerçant excédant le solde disponible et considèrent que dans ce dernier cas, l'auteur se rend coupable d'escroquerie [12] ou d'abus de confiance [13].

En Belgique, d'aucuns considèrent que les conditions du vol sont réunies [14], alors que l'escroquerie est retenue par d'autres [15]. Enfin, certains y voient un cel frauduleux [16].

1.1.2. Utilisation frauduleuse d'une carte annulée ou périmée

Une minorité d'auteurs distinguent l'utilisation d'une carte annulée de celle d'une carte périmée [17]. D'après eux, l'utilisation d'une carte périmée ne constituerait pas une escroquerie sauf en tant que carte de garantie de chèque [18] alors que l'utilisation d'une carte annulée pourrait être qualifiée de tentative de vol lorsqu'elle vise à utiliser un distributeur automatique de billets et d'abus de confiance lorsqu'elle vise le réglement d'achats chez un commerçant [19]. Cette dernière hypothèse a été qualifiée d'abus de confiance par le tribunal de Créteil [20]alors qu'il s'agissait d'une

escroquerie pour le tribunal de Paris [21].
La majorité des auteurs analysent l'utilisation de la carte périmée ou annulée de façon identique. L'incrimination d'escroquerie est retenue largement par la doctrine [22].
Certains y voient aussi un abus de confiance car en règle générale, le titulaire de la carte s'engage à la restituer à l'émetteur à la première réquisition en vertu d'une convention de prêt à usage [23].

1.1.3. Utilisation d'une carte obtenue frauduleusement

La qualification d'escroquerie dépend de la façon dont le titulaire s'y est pris. Se contente-t-il d'un mensonge (verbal ou écrit), le fraudeur ne se rend pas coupable d'escroquerie. Si le fraudeur organise une mise en scène, l'infraction peut être établie [24].
Si la carte a été obtenue au moyen d'un formulaire de demande de carte comprenant à dessein des données inexactes, on pourra éventuellement retenir un faux en écriture [25].

1.1.4. Utilisation de la carte postérieurement à la déclaration de sa perte ou de son vol

Cet agissement peut être qualifié d'escroquerie [26].

1.2. L'auteur est un porteur illégitime

Deux types de fraude sont constatées : l'utilisation d'une carte perdue ou volée (1.2.1.Utilisation d'une carte perdue ou volée) et l'utilisation d'une carte falsifiée (1.2.2.Utilisation d'une carte falsifiée).

1.2.1. Utilisation d'une carte perdue ou volée

Ce comportement est unanimement considéré comme étant une escroquerie [27]. La doctrine est divisée sur la thèse du vol [28]. La thèse de l'usurpation de nom (art. 231 C.P. belge) est également avancée [29]. On signalera enfin que l'hypothèse rentre dans le champ d'application du nouveau § 263 a du Code pénal allemand.

1.2.2. Utilisation d'une carte falsifiée

Ce comportement se dédouble juridiquement en deux temps : la confection d'un faux en écriture [30] ou de contrefaçon de titres (art. 144 C.P. français) [31] et l'usage de la carte falsifiée qui s'analyse en un délit d'usage de faux (art. 151 C.P. français)[32] ou en une escroquerie [33].

2. Fraudes opérées sans l'aide d'une carte

Les transferts électroniques de fonds consistent en des transmissions de messages sur des réseaux de télécommunications. La première partie concernait les fraudes perpétrées aux terminaux avec l'aide d'une carte. On peut envisager le cas de fraudes commises aux terminaux sans l'aide d'une carte par le trucage de l'appareil automatique, conduisant à la remise de fonds ou à l'inscription au crédit d'un compte (par exemple en manipulant le logiciel ou en trafiquant le système de commande). On peut voir dans ces comportements des mesures frauduleuses constitutives d'une escroquerie 34. Lorsque le truquage a porté sur les données d'input et/ou les logiciels, la question se pose de savoir si la manipulation peut être considérée comme étant la fabrication d'un faux en écriture. La plupart des auteurs doutent que les supports contenant ou transportant des données informatiques puissent être considérés comme des écrits au sens de la loi pénale [35]. Une évolution dans le sens de l'assimilation semble se dégager en jurisprudence [36]. Lorsque la manipulation de données implique la suppression de certaines d'entre elles, on pourrait songer à l'incrimination de vol. Cette qualification est très problématique en raison du caractère incorporel des données informatiques[37]. Ce comportement est puni en droit allemand par le § 263 a ("Computer-betrug").
Le transport du message relatif au transfert de fonds se prête également à des fraudes. Les réflexions menées relativement aux manipulations de données et de logiciels au niveau du terminal valent également pour les manipulations opérées au niveau de la transmission.

La manipulation d'information n'est techniquement pas nécessaire pour frauder sans l'aide d'une carte. On peut notamment songer à l'utilisation d'un code d'accès secret percé lors d'une "écoute" de la communication. Cette fraude s'analyse en deux temps. Le fraudeur a d'abord "écouté" la communication ; ensuite, il a fait usage du code découvert. Le premier

comportement rentrera dans le champ d'application du droit pénal des télécommunications pourvu que la technique de transmission utilisée corresponde à la lettre de la loi. La plupart des Etats prohibent la prise de connaissance ("l'écoute"), la soustraction, la distraction, la suppression, le fait d'avoir gêné des correspondances téléphoniques, télégraphiques ou hertziennes [38]. Or, les messages transitent généralement sur le réseau téléphonique et sont des correspondances téléphoniques.

Le second comportement, parfois considéré comme constitutif de manœuvres frauduleuses caractéristique de l'escroquerie [39], est également vu comme la prise d'un faux nom ou d'une fausse qualité. Enfin, il est à noter que la réforme allemande du droit pénal économique règle spécifiquement la question en créant une incrimination spécifique [40].

Notes du chapitre VIII

[1]On dispose de peu de chiffres publiés relatifs à ce phénomène. Les préjudices résultant d'utilisations frauduleuses de cartes de crédit sont mieux connus : W. JEANDIDIER, o.c., note (10) cite le chiffre de 32 millairds de francs français de dommages en 1984 pour les institutions financières du monde entier.

[2]Cfr. notamment J.M. DU PEYROUX, "Electronic Banking : évolution dans les dix prochaines années", p. 5 ; Conférence "Electronic Banking : les défis de la banque de demain dans le contexte juridique d'hier" organisé à Bruxelles les 9 et 10 mars 1987.

[3]C. ERKELENS, "La délinquance informatique et le droit pénal belge", Droit de l'Informatique, 1985/6 (Dossier Fraude Informatique), 21 ; R. GASSIN, "Le droit pénal de l'informatique", Recueil Dalloz - Sirey (chronique), 1986, 42; G. DEMANET, "De l'utilisation frauduleuse des cartes bancaires. Une nouvelle incrimination est-elle nécessaire ?", Revue de droit pénal et de criminologie, 1985, 930 qui plaide pour l'adoption d'une loi commune ou d'une loi uniforme au niveau européen.

[4]Supra chap. VI.

[5]Le problème de l'effectivité des normes souhaitées est rarement envisagé par les partisans d'une modification de la loi.

[6]Loi du 6 juin 1985 relative à l'escroquerie informatique (traduction française dans Droit de l'Informatique, 1985/6, 49

[7]Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. Wikg) du 15 mai 1986.

[8]Proposition de loi relative à la fraude informatique, Document n° 352 (Assemblée Nationale) ; projet de loi portant réforme du Code pénal, Document n° 100 (Sénat), Annexe au procès-verbal de la séance du 20 février 1986.

[9]. § 266 b al. 1 du Code pénal allemand.

[10] En faveur de la thèse du vol, Corr. Troyes, 27 avril 1976, D., 1977, I, 122, not. Cazal ; Lyon, 20 avril 1982, D., 1977, 538, note B. SOUSI-ROUBI. En faveur de la thèse de l'escroquerie, Douai, 10 mars 1976, Rev. Trim. dr. Comm., 1976, 584, obs. CABRILLAC et RIVES-LANGE.

[11]. Cass. fr., 24 novembre 1983, J.C.P., 1985, II, 20450, note CROZE ; cfr. aussi Angers, 2 décembre 1980, Revue de science criminelle, 1982, 129, obs. BOUZAT, Lyon, 9 juillet 1981, Gaz. Pal., 1981, II, 204, note B.

de cartes magnétiques", J.C.P. 1986, I, 3229.

18. W. JEANDIDIER, o.c., n° 16

19. W. JEANDIDIER, o.c., n° 18

20. Trib. Gr. Instance de Créteil, 15 janvier 1985, D., 1985, I.R., 344 ; Trib. Corr. Paris 16 octobre 1974, J.C.P., 1976, 12-219.

21.

22. GAVALDA et STOUFFLET "Droit bancaire (chronique), J.C.P., 1976, I, 2801, n° 83 ; A. MASSET, o.c., 141.

23. A. MASSET, o.c., 141

24. A. MASSET, o.c., 140

25. A. MASSET, o.c., 140

26. J. DEVEZE, o.c., n° 9 ; W. JEANDIDIER, o.c., n° 7.

27. J. DEVEZE, o.c., n° 9 ; C. ERKELENS, o.c., 23 ; A. MASSET, o.c., 139 ; W. JEANDIDIER, o.c., n° 12 ; dans l'hypothèse d'un paiement à un commerçant (T.P.V.) paris, 22 février 1975 et Paris 2 février 1977 inédits cités par B. SOUSI-ROUBI, "Les cartes, Panorama de jurisprudence", Les petites affiches, 15 septembre 1986, n° 111, 91 et Paris, 11 février 1977, D., 1982, I.R. 500, obs. M. VASSEUR ; dans l'hypothèse de retraits de billets (distributeurs automatiques de billets) Rennes, 26 janvier 1981, D., 1982, I.R. 500, obs. M. VASSEUR et Trib. Corr. Paris, 13 janvier 1982, Expertises, n° 40.

28. Considèrent qu'il y a vol (à l'aide de fausses clefs) J. DEVEZE, o.c., n° 9; C. ERKELENS, o.c., 22-23 (en tous cas s'agissant de l'utilisation de distributeur automatique de billets) ; J.P. SPREUTELS, o.c., 367 (pourvu que l'expression "fausses clefs" soit interprétée largement) ; Corr. Hasselt, 26 octobre 1984 inédit cité par G. VANDENBERGHEet J. de LAME, o.c., 283 ; contra A. MASSET, o.c., 138 Cor.

29. C. ERKELENS, o.c., 23.

30. J. DEVEZE, o.c., n° 9, W. JEANDIDIER, o.c., n° 10 qui précise qu'en cas de falsification des seules pistes magnétiques, le faussaire ne peut être prévenu de faux en écriture car la notion d'écrit suppose un support constitué de signe visible ; R. GASSIN "Le droit pénal de l'informatique", Dalloz, (chronique) 1986, 40 ; "Rapport du conseil National français du Crédit sur les nouveaux moyens de paiement", 9.

31. MARLY et CABRILLAC, cités par W. JEANDIDIER, o.c., n° 10.

32. W. JEANDIDIER, o.c., n° 12 ; R. GASSIN o.c., 40 ; Rapport du CNC, o.c., 9.

33. W. JEANDIDIER, o.c., n° 12 ; R. GASSIN o.c., 40.

34. A. MASSET, o.c., ; C. ERKELENS, o.c., 24 ; R. GASSIN, o.c., 39 ; JAEGER, "

La fraude informatique", Revue de droit pénal et criminel, 1985, 344, sous la réserve qu'une (ré)action humaine lui paraît nécessaire à un quelconque stade du processus.

35. R. GASSIN, o.c., 40.

36. Voyez J.P. SPREUTELS, o.c., 366.

37. JAEGER, o.c., 342.

38 Article L 42 du Code français des P.T.T. ; article 616 du code pénal italien ; article 17 de la loi belge du 23 octobre 1930 ; § 202a du code pénal allemand.

39. J.P. SPREUTELS, o.c., 366

40. § 263 a du Code pénal.

IX LES TRANSFERTS ELECTRONIQUES DE FONDS ET LE PROBLEME DES LIBERTES

Evoluant vers une monnaie abstraite, le commerce de l'argent met en oeuvre des traitements d'information nombreux et rapides. De là, le spectre de la menace pour la vie privée que suscite toujours l'informatique. Plus que tout autre peut-être, le traitement d'informations relatives à ce moyen universel d'échange qu'est la monnaie permet un contrôle social de l'individu risquant de mettre en péril des libertés fondamentales telles celle de se déplacer, la liberté d'opinion, la liberté choisir des produits, la liberté d'obtenir du crédit, la liberté de consommer etc .. (1. Protection de la confidentialité des données à caractère personnel).

Les transferts électroniques de fonds risquent aussi de porter atteinte à la liberté de choix des moyens et services de paiement et des prestataires de ces services (2.1. Liberté du choix des moyens de paiement).

Enfin, il ne faudrait pas que certaines catégories de personnes soient oubliées dans les plans de développement des services de transferts électroniques de fonds. Il y va de la liberté d'accès au progrès technique (2.2. L'accès aux services de T.E.F.).

1. Protection de la confidentialité des données à caractère personnel

A priori, on pourrait croire que la problématique de la vie privée dans les transferts électroniques de fonds. ne présente aucune spécificité par rapport aux autres applications informatiques ou télématiques. C'est par exemple ce qu'estime le Groupe de travail australien examinant les problèmes juridiques suscités par les transferts électroniques de fonds[1]. On observera d'abord que certains dangers sont particuliers aux services télématiques. Songeons par exemple aux possibilités qu'offre la télématique de connaître les moments d'interrogation, les moments de présence à domicile, les pôles d'intérêt, etc.

L'Allemagne, qui connaît les réglementations fédérales et des Länder concernant la protection des données, dispose également d'une

réglementation spécifique au Bildschirmtext comprenant notamment des dispositions particulières aux problèmes "privacy" [2]. Le rapport de l'Office of Technology Assessment est explicite sur les craintes que suscitent les transferts électroniques de fonds. " 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 online, 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 facilitated, it will be more difficult for corrections to catch up with and replace faculty information" [3].
Ces dangers apparaissent clairement lorsqu'on considère les types de données traitées et le transit des données.

1.1. Les données traitées et créées

Les critères de classification des données sont multiples. On en adopte deux : le critère chronologique et celui de la fonction.
D'un point de vue chronologique, on distingue les données avant le traitement, celles créées lors du traitement et enfin, celles créées postérieurement à celui-ci. Jusqu'à présent, les législations vie privée se sont principalement centrées sur les données créées a priori, antérieurement à l'utilisation d'un service. Or, ce sont celles créées lors de l'utilisation du service et par celle-ci qui permettent un contrôle social important. Quant à celles créées postérieurement à l'utilisation du service, elles se retrouvent principalement dans les configurations off-line et dans les services de transferts électroniques de fonds. prestés par des entreprises non-bancaires (facturation).

Du point de vue de la fonction, on distingue les données de transmission nécessaires à l'acheminement du message, celles relatives à la gestion (ex. N° de compte, code d'accès, n° d'un éventuel bénéficiaire, etc...) et celles relatives à la transaction. Si les premières sont peu dangereuses, les secondes le sont davantage dans la mesure où elles permettent d'identifier. Elles le sont davantage encore lorsqu'elles sont combinées aux troisièmes, les plus dangereuses.

On remarquera que ces données ne concernent pas exclusivement l'utilisateur mais parfois également des tiers (bénéficiaire d'un transfert

électronique de fonds).

1.2. Le transit des données

Les données créées par l'utilisation des services de transferts électroniques de fonds. sont acheminées et traitées en de multiples endroits et chez de multiples intervenants. Aux intervenants dans le schéma le plus simple (banque-client) s'en ajoutent d'autres qu'expliquent la structure institutionnelle bancaire (transit par des chambres de compensation), la complexité technique de l'opération (d'où l'intervention de services spécialisés) et les services annexes offerts par les prestataires de service de transferts électroniques de fonds. (ex. relevés mensuels d'achat de carburant). Comme pour les autres applications informatiques, une approche souple du problème est préférable à une interdiction a priori de certaines données. C'est que différents acteurs ont des intérêts divers, parfois légitimes au regard de la collecte, du traitement, de la conservation et de la communication de certaines données relatives aux transferts électroniques de fonds.

1.3. Les intérêts des personnes concernées par ces données

Le *fournisseur du service* d'abord, a intérêt au stockage de certaines informations nominatives relatives à la transaction à des fins d'exécution de l'opération (ex. rapport avec une chambre de compensation), de preuve (maintien d'une trace de l'opération) non seulement vis-à-vis du client mais aussi au regard des lois comptables et fiscales et de gestion rationnelle (une comptabilité analytique lui permet d'évaluer la rentabilité de certains types d'applications, de mieux connaître le profil du client "intéressant", le crédit de ses clients et sa propre entreprise). Dans le cas de T.P.V., le *commerçant* a mutatis mutandis les mêmes intérêts que ceux évoqués. On remarquera toutefois que les facilités de gestion qui peuvent découler de l'installation des T.P.V. ne bénéficient pas nécessairement à tous les commerçants. On a déjà relevé qu'un T.P.V. peut constituer une charge administrative supplémentaire dans la mesure où le commerçant doit en fin de journée, procéder à la réconciliation comptable des transactions payées en monnaie liquide, par chèque et par T.P.V.

Dans le cas d'un transfert électronique de fonds. autre que celui réalisé à son propre profit ou au profit d'un commerçant, c'est-à-dire au profit d'un

tiers bénéficiaire, celui-ci peut craindre que ses sources de revenus soient identifiées.

Quant à l'*utilisateur*, ses libertés peuvent être affectées par le traitement, le stockage et la transmission à des tiers de données relatives à la transaction. En effet, il est possible d'en inférer ses habitudes de consommation par ses achats, ses déplacements, ses opinions (abonnement à un journal, paiement d'une cotisation syndicale) la façon dont il gère son budget et ses avoirs. Son désir de garder l'anonymat pour certaines opérations (ex. donation) ainsi que ses possiblités d'obtenir du crédit (suite à l'enregistrement du dépassement répété de la provision ou suite à un credit scoring) ou encore l'accès à un certain service suite à un ciblage de clientèle, peuvent être affectés.

Par contre, l'utilisateur aura intérêt à la conservation et au traitement des informations à des fins de preuve vis-à-vis d'un commerçant par exemple ou vis-à-vis de l'administration fiscale, pour gérer son budget (une comptabilité analytique domestique se concevrait si la pratique des relevés mensuels comme cela existe notamment en Belgique s'agissant des dépenses de carburant, était généralisée). Enfin, s'agissant plus particulièrement de la banque à domicile, l'utilisateur peut avoir intérêt à la mémorisation de certaines informations afin de ne pas devoir recommencer le dialogue télématique à partir du début.
L'*administration* et plus particulièrement l'administration fiscale a intérêt à pouvoir accéder à certaines données afin de contrôler tantôt les commerçants tantôt les utilisateurs.
Enfin, la production devant le *juge* de certaines données peut présenter un intérêt lorsque l'opération de transfert électronique de fonds. elle-même est contestée ou s'agissant d'affaires étrangères à l'opération en tant que telle (ex. affaires pénales).

1.4. Les réglementations en vigueur

A l'exposé des réglementations générales applicables à la matière fait suite un examen des solutions spécifiques. Parmi les réglementations générales, on relève les principes généraux dégagés au niveau international par la Convention du Conseil de l'Europe du 17 septembre 1980 et au niveau national par certaines législations "vie privée", les règles de secret

bancaire et celles applicables au secret des télécommunications.

1.4.1. Les principes dégagés par les réglementations sur la vie privée

1.4.1.1. Le principe de pertinence

La Convention du Conseil de l'Europe du 17 septembre 1980 entrée en vigueur le 1er octobre 1985 entre l'Espagne, la France, la Norvège, la République fédérale d'Allemagne et la Suède et qu'ont signée une quinzaine d'Etats consacre certains principes. Au premier rang de ceux-ci, le principe de l'adéquation des données par rapport au traitement, principe d'après lequel les données doivent être obtenues, traitées, conservées et communiquées légalement en fonction des finalités déterminées a priori (article 5 de la Convention). Ce principe a été affiné par le Bildschirmtext Staatsvertrag allemand concernant notamment les transferts électroniques de fonds par Bildschirmtext (v. infra).
L'application du principe de pertinence devrait conduire notamment à imposer au prestataire du service ainsi d'ailleurs qu'aux autres intervenants de préciser les finalités des traitements, les données qu'ils présupposent, la durée de leur conservation ainsi que les destinataires de leur communication.

1.4.1.2. Le principe du droit d'accès

Ce principe a pour but d'assurer à la personne concernée une transparence des données et des traitements (article 8 de la Convention). Il présuppose actuellement une information sur l'existence même de ces traitements et des personnes responsables. Lors de l'utilisation des services de transferts électroniques de fonds, certaines données sont communiquées et traitées (notamment celles incorporées aux cartes d'accès) et d'autres relatives à la transaction sont créées.

1.4.1.3. Le principe du droit de rectification

Ce principe permet à l'intéressé d'exiger que soient rectifiées, complétées, clarifiées ou mises à jour des données inexactes, incomplètes, ambigues ou périmées (article 8 de la Convention).

Cette question peut avoir son importance lorsque les données concernant

l'utilisateur mentionnent erronément que celui-ci a dépassé abusivement son avoir disponible, ou qu'il a été négligent dans la conservation du code secret ce qui peut porter atteinte à sa liberté d'obtenir du crédit ou entraîner le retrait de ses moyens d'accès.

1.4.1.4. Le principe de l'interdiction des décisions ayant pour fondement unique un traitement automatisé donnant une définition du profil de l'utilisateur

Cette règle consacrée par l'article 2 de la loi française "Informatique, fichiers et libertés" devrait conduire à interdire le refus ou le retrait de moyens d'accès et le refus d'un crédit sur base d'un ciblage de clientèle ou d'un "credit scoring" s'appuyant sur des données créées lors de l'utilisation de services de transferts électroniques de fonds.

On s'accordera toutefois à reconnaître que la règle, pour intéressante qu'elle soit, est d'une effectivité incertaine.

1.4.1.5. Le principe des moyens de sécurité suffisants

1.4.1.6. Les règles protectrices des télécommunications

On sait que les Etats se sont généralement dotés de règles visant à protéger le secret des télécommunications. Ce principe a également été affirmé au niveau international par la Convention internationale des télécommunications.
Les transferts électroniques de fonds supposent naturellement le transport d'informations par des procédés de télécommunications et sont donc protégés par ce biais.

1.4.2. Le secret bancaire

Si le principe du secret bancaire a été consacré expressément par des textes pénaux ou constitutionnels dans certains Etats, la jurisprudence des Etats européens dégage généralement 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 tandis que selon un courant doctrinal et certaines décisions de justice, cette obligation relève du secret professionnel pénalement sanctionné [4].

Il est évident que le secret bancaire ou a fortiori l'obligation de discrétion, cèdent devant certaines personnes ayant droit à la divulgation du secret (ex. autre banquier chargé d'exécuter l'opération par le banquier du client non en mesure de l'exécuter lui-même, mandataire ayant reçu pouvoir d'opérer sur le compte, représentant légal d'un incapable, héritiers et légataires universels, certaines autorités monétaires, administration fiscale dans certains cas, juge pénal). Dans un système électronique de transfert de fonds, certaines informations protégées par le secret ou l'obligation de discrétion (ex. mouvements du compte, montant, ...) sont inévitablement transmises sur des réseaux appartenant à des tiers à la banque (transporteurs d'informations, commerçants propriétaires de T.P.V., société de services techniques, ...). Le secret bancaire ne peut évidemment avoir pour effet d'empêcher le développement de nouveaux modes de transmission d'ordres bancaires. La question se pose de savoir quelle est à cet égard l'étendue de l'obligation du banquier [5].
Le secret bancaire ne s'étend pas à toutes les informations. Il est par exemple d'usage d'admettre la communication à un client d'appréciations générales sur la solvabilité d'un contractant potentiel [6].

1.4.3. Réglementations spécifiques

14.3.1. La législation allemande

L'article 9 du Btx-Staatsvertrag spécifie le principe général de pertinence. La mise en oeuvre de ce principe est équilibrée et souple. Certaines données sont exclues a priori (le § 3 précise que l'intégrateur - en l'espèce la Deutsche Bundespost - ne peut collecter, traiter et stocker que les données relatives à la facturation et ces données sont précisées ainsi que les cas où elles peuvent être communiquées à des tiers) mais d'autres sont autorisées en fonction de l'adéquation à la finalité du traitement. Cette finalité conduit à n'autoriser la collecte de données que dans la mesure où elles sont nécessaires à l'exécution de la prestation où à la formation d'une relation contractuelle (§ 6). Il en est de même de la communication de ces données à des tiers. On le devine, cette règle risque d'avoir pour effet que les prestataires de services cherchent à formuler différemment les contrats pour que soient justifiés la collecte et le traitement de certaines données au regard de l'objet du contrat [7].

1.4.3.2. La législation danoise

C'est la même perspective qu'a adoptée le législateur danois. L'article 24 de la loi sur les cartes de paiement dispose que, sauf disposition légale contraire, seules les informations concernant le porteur de la carte nécessaires à l'exécution des transactions de paiement et à l'établissement d'un fichier des cartes perdues ou utilisées abusivement peuvent être enregistrées, utilisées et communiquées. Les informations relatives aux usages abusifs ne peuvent être communiquées que pour autant qu'elles soient nécessaires à la prévention d'autres abus.

Le paragraphe 3 de cet article consacre la même règle s'agissant des informations concernant le bénéficiaire du paiement (sous réserve bien sûr des informations relatives aux usages abusifs des cartes).

La durée de conservation des données est limitée à cinq années sauf celles relatives aux usages abusifs qui doivent être détruites après deux ans.

1.5. Conclusions et pistes de réflexion

Le problème a encore été insuffisamment été aperçu jusqu'à présent. Une tendance se dessine favorable à une adaptation des législations en vigueur. Les législations relatives à la vie privée développées jusqu'ici se centraient principalement sur les données créées avant la création du service. Les services télématiques en général et particulièrement les transferts électroniques de fonds. suscitent des craintes s'agissant des données créées par l'utilisation du service.

Les réglementations générales telle la Convention du Conseil de l'Europe contiennent des principes intéressants qui mériteraient d'être adaptés aux transferts électroniques de fonds.

Les législations spécifiques existantes sont encore insuffisantes :
1. Quant au principe de pertinence, sa mise en oeuvre en fonction de l'exécution des transactions de paiement ou des contrats (ex. contrat de services transferts électroniques de fonds.) renferme des risques d'effets pervers (voir supra p. 1.4.3.1.).

2. Quant à la collecte des données, l'application du principe de pertinence devrait conduire à déterminer a priori les informations autorisées à être collectées notamment sur la carte et particulièrement sur la carte à mémoire surtout si elle est multifonctionnelle. Mais la question se pose de savoir qui procède à la collecte de quelles données. S'il ne fait aucun doute que l'émetteur de la carte enregistre les données de gestion nécessaires avant l'utilisation du service (v. supra IX 1.1.), le doute apparaît s'agissant des données relatives à la transaction, c'est-à-dire celles créées lors de l'utilisation du service : le commerçant et la banque au moyen de leur infrastructure activée par eux-mêmes collectent certaines d'entre elles. Certaines de ces informations sont ensuite communiquées à l'éventuelle entreprise émettrice (société de cartes de crédit ou entreprise de distribution). Le fait que le porteur de la carte transporte lui-même ces informations (mémorisées dans la carte) ne change pas les données du problème [8]. Par contre, s'agissant des cartes à mémoire autonomes (comprenant clavier et écran), ce n'est plus l'appareillage du commerçant et de la banque activé par eux qui assure la saisie des informations mais bien la carte du porteur activée par ce dernier.

3. Quant à l'accès aux données et aux procédures de traitement de celles-ci, la transparence au niveau des circuits empruntés par les données et des acteurs impliqués devrait être assurée.

4. Quant à la conservation des données, leur durée devrait être limitée et précisée. Cette règle implique une harmonisation avec les lois fiscales et comptables d'une part et avec les règles de responsabilité si les recours sont limités dans le temps (v. supra).

5. Enfin, quant à la technique mise en oeuvre, une obligation d'adaptation au progrès technique devrait être imposée qui viserait à garantir certaines mesures techniques de sécurité.

2. La liberté du choix des moyens de paiement

L'O.T.A. américain, sur le thème "Equity in Electronic Funds Transfer" (Rapport cité plus haut) esquissait ainsi la problèmatique : "In modern society, it is essential for individuals, households, and businesses to have

a mechanism for carrying out basic economic transactions (such as paying for necessary goods and services). Therefore, it is important that no segment of society-especially these already disadvantaged, such as the low-income groups or the physically handicapped is deprived of a reliable means of making and collecting payments" et il concluait : "There appear to be few reductions in equity inherent in EFT systems for socially disadvantaged groups, as long as a full range of alternative payment systems and financial service delivery systems continue (...). However, in the future, if EFT displaces conventional alternatives in certain neighborhoods, communities, or regions (or replaces them completely), socially disadvantaged groups may suffer significant additional restrictions on their ability to function in society".

La liberté de choix du consommateur face aux moyens de paiement doit être affirmée sous trois angles : la liberté de choix suppose le maintien des moyens de paiement traditionnels (2.1.) mais suppose aussi l'accès aux nouveaux procédés (2.2.). Ces libertés garanties, le choix n'est qu'un leurre si la structure de l'offre n'est pas concurrentielle. Ce dernier aspect sera abordé sous l'angle du droit européen de la concurrence dans le chapitre suivant.

2.1. Le maintien des moyens de paiement traditionnels

Téléphoner à une connaissance lorsqu'on arrive dans certains pays devient de plus en plus malaisé. Les téléphones à monnaie ont largement cédé la place aux téléphones fonctionnant avec des cartes valeur. Cet exemple illustre un désagrément parmi d'autres [9]. que risque d'entraîner le développement des nouveaux moyens de paiement s'il devait avoir pour conséquence de supprimer les moyens de paiement traditionnels. La crainte d'une atteinte à l'anonymat (ex. dans le cas d'une donation), celle de l'atteinte à la vie privée, le refus d'une déshumanisation des transactions sont d'autres raisons légitimes de préférer d'autres procédés de paiement que les transferts électroniques de fonds. Autre raison également, le souci d'être freiné dans une propension à consommer (effet psychologique de frein que procure chez certains la dépossession d'argent liquide), la peur d'être négligent dans la conservation de documents n'ayant pas de valeur en soi (telle la carte magnétique). Le choix peut également être guidé par les conséquences juridiques qui s'attachent à tel ou tel mode de paiement (ex. suites pénales de l'émission sans provision

suffisante, irrévocabilité du paiement par carte de paiement en France, contrôle du moment du paiement, ...).
Pour être complet, on notera également que certaines personnes âgées, vu leur mémoire et leur acuité visuelle défaillantes ainsi que leur faible degré de familiarisation avec les nouvelles techniques, craignent d'être victimes de fraudes, notamment lorsqu'elles demandent de l'aide à des inconnus. De plus, les aveugles et les dyslexiques souhaitent que d'anciens services de paiement restent disponibles. Si le problème des premiers peut être résolu par l'installation de claviers en braille, celui des seconds le serait par des dispositifs de réponse vocale.

La crainte existe de voir les institutions financières promouvoir l'installation systématique des G.A.B. et T.P.V., vu les avantages que présentent pour elles ces systèmes. Si le réseau d'agences venait à disparaître, nombreuses seraient les personnes privées d'un service personnalisé. Si des avantages d'ordre tarifaire ou autres étaient accordés à ceux qui paient par transferts électroniques de fonds, le choix entre les moyens de paiement serait un leurre. Si enfin, certains débiteurs forçaient leur créancier à accepter les paiements par T.E.F., ces personnes peut être peu enclines à traiter avec les banques se verraient contraintes à ouvrir un compte auprès de l'une d'elles (exemple cité par l'OTA qui évoque le cas d'employeurs exigeant que les salaires soient payés directement sur des comptes de dépôt et esquisse la possibilité que les paiements effectués par l'administration soient versés directement sur un compte de dépôt).

La loi danoise comprend certaines dispositions visant à garantir la liberté du choix entre moyens de paiement. Outre, l'interdiction de l'envoi forcé d'une carte, la loi dipose en son article 17 :"When required goods or services by means of a payment card, the card holder shall not be granted a rebate or a similar advantage unless the same advantage is granted for payment in cash."

La crainte d'une discrimination entre le paiement par carte et le paiement par argent liquide se fonde sur le constat de la pratique de certains distributeurs qui consiste à accorder une ristourne au porteur d'une carte accréditive qui paie comptant en liquide. Cette pratique s'explique par la commission que le commerçant doit verser à l'organisme émetteur et dont il peut ainsi faire l'économie partielle. Cette situation est évidemment

transposable aux T.E.F.

Et l'article 18 oblige le créancier à accepter les paiements en argent liquide : "The payment creditor shall accept payment in cash within normal business hours in settlement of payment obligations which could be entered into and fulfilled by means of a payment card".

En outre, certaines dispositions générales de droit monétaire accordent à la monnaie ayant cours légal un cours forcé.

Un accord semble se dégager chez les auteurs et décideurs pour que soit maintenue la possibilité d'un choix neutre entre différents services de paiement. En définitive, comme le note l'O.T.A. américain, il faut que les consommateurs soient suffisamment informés, de sorte qu'ils soient à même de comprendre les avantages et inconvénients des différents procédés et de choisir ce qu'ils estiment être l'optimum pour eux. Le rapport énonce : "Consumer education is required, and many providers of financial services and other agencies are beginning to furnish it. Consumers need to become familiar with five aspects of financial services:
1. costs ;
2. the mechanism of using such services ;
3. the benefits that are offered ;
4. the obligations and responsibilities that are accepted when participating in each service, such as the ways to safeguard one's own account (e.g. discretion in use of personal identification number) ; and
5. their rights as consumers, and especially the methods for identifying, challenging and correcting errors" [10].

2.2. L'accès aux services de T.E.F.

Si les formes traditionnelles de paiement présentent des avantages par rapport aux T.E.F., ces derniers en procurent d'autres par rapport aux premiers. Le partage de ces avantages entre le plus grand nombre est la question envisagée ici.

Les avantages des services de T.E.F. pourraient être largement partagés si les fournisseurs de ces services prêtaient une attention aux besoins de certaines catégories de personnes. On songe par exemple aux personnes

vivant dans des régions reculées, ou des personnes ayant peu de contact social. L'installation de G.A.B. et de T.P.V. et plus encore le home banking est susceptible de permettre à ces personnes d'éviter de se déplacer et de favoriser leur indépendance dans la gestion de leurs affaires. On songe aussi aux aveugles pour lesquels l'adjonction d'un dispositif nasal ou de touches en braille favoriserait leur accès à ces services.
De façon générale, il faut éviter que ne se crée une discrimination entre ceux qui bénéficient des nouveaux moyens de paiement et ceux qui, pour des raisons diverses, n'en bénéficient pas.

Enfin, se pose la question des coûts des services de T.E.F. Comment vont-ils être partagés ? Le développement des T.E.F. va-t-il réagir sur le coût des services traditionnels de paiement ? Ces deux questions ne sont pas de notre compétence et nous ne pouvons donc que les soulever ici.

Vu l'intérêt des banques à développer les services de T.E.F., vraisemblablement les utilisateurs ne subissent-ils que peu la charge des investissements nécessaires. S'agissant des bénéficiaires, la loi danoise interdit le report automatique des frais afférents à l'utilisation des services de paiement par carte sur le créancier [11].

Notes du point IX

[1] Second Report of the Working Group Examining the Rights and Obligations of the Users and Providers of Electronic Funds Transfer Systems, Australian Government Publishing Service, Canberra, 1986, p. 26 ; ce chapitre s'inspire pour une large part de l'étude faite par Y. Poullet Telebanking and Privacy in Telebanking, Teleshopping, Legal Aspects, Y. POULLET, G. VANDENBERGHE (Drs), Kluwer, Amsterdam, à paraître.

[2] Article 9 du Bildchirmtext Staatsvertrag du 18 mars 1983.

[3] Office of Technology Assessment of the Congress of the United States of America, Selected EFT Issues : Privacy, Security and Equity, 1982, 29 ; cfr. aussi Th. KAISER, Legal implications of automated teller machines, London School of Economics, June, 1985, p. 96 et s.

[4]- Tournier v. National Provincial and Union Bank of England (1 k. B. 461)
- BGH, 4 mars 1973
- Paris, 6 février 1975, D. 1975, 318 note J. Vezin
- Cass. belge, 25 octobre 1978, J.T., 1979, 371, note A.Bruyneel
- G. MOLLE, I contratti bancari, Giuffrè, 1978, pp. 68 et s. citant Cass., 10 juillet 1974, 2197.

[5] R. SCHWEIZER, "La protection des données et autres problèmes juridiques des nouveaux moyens électroniques de paiement, Les nouveaux moyens de paiement, Collection juridique romande, Payot, Lausanne, 1986, p. 52.

[6] C. GAVALDA et J. STOUFFLET, Droit de la banque, P.U.F., Coll. Thémis, Paris, 1974, p. 396 citant Trib. civ. Strasbourg, 28 avril 1954 ; Banque, 1954, 304 obs. Marin.

[7] La parade semble assez classique.

[8] R. HARTSTEIN, Der Datenschutz bei Bildschirmtext, in Das Bildschirmtext Recht entwickelt sich, Bildschirmtext - Anbieter - Vereinigung, Berlin, 1985, p. 52.

[9] LE CLECH, Ph., "Le droit des cartes à mémoire bancaires", D.I.S.E.P., septembre 1985, 5

[10] Rapport cité, p. 60, 63 et 67

[11] Article 20 de la loi sur les cartes de paiement

X. DROIT DE LA CONCURRENCE

D'abord seront énoncées les raisons faisant craindre une restriction de la concurrence (1 Raisons de la crainte d'une restriction de la concurrence).
Ensuite, la position de la Commission sera analysée s'agissant d'une problématique proche de celle des services de T.E.F., à savoir la décision Eurochèque (2. La décision Eurochèque).
Enfin, le raisonnement sera transposé autant que faire se peut, aux T.E.F. (3. Application aux T.E.F.).

1. Raisons de la crainte d'une restriction de la concurrence

La crainte d'une réduction de la structure concurrentielle de l'offre des systèmes de T.E.F. a été largement exprimée. Elle se fonde sur des situations antérieures concernant d'autres moyens de paiement, plus particulièrement les services de cartes de crédit. Comme pour les cartes de crédit, le succès des T.E.F. dépend de l'étendue et de l'organisation du réseau des participants. Plus encore que pour les systèmes de crédit, la normalisation se justifie pour des raisons techniques, économiques et commerciales.

Raisons techniques d'abord. Il est évident qu'un T.E.F. présuppose que le donneur d'ordre et le bénéficiaire adhèrent à un même système dont les équipements sont techniquement compatibles (matériel, protocoles de télécommunications, etc.). A cet égard, on note l'action des Communautés Européennes en vue d'une normalisation technique des équipements (v. infra chap. XI). Il est évident qu'une normalisation technique implique des accords entre banques et entre banques et commerçants. D'une normalisation technique, on ne peut inférer une restriction de concurrence. Au contraire, la normalisation technique permet à un plus grand nombre d'institutions financières et de commerçants d'adhérer au système, diminuant le risque des clientèles captives d'un fournisseur. Un bon exemple est fourni par la télématique interactive en France. L'intégration technique du réseau Télétel (et la politique volontariste de l'Administration des télécommunications) a permis le développement de toute une industrie télématique, où la concurrence joue pleinement.
Bref un accord sur les techniques ne porte pas préjudice en principe à la

concurrence entre les services offerts qui doit être maintenue.

Raisons économiques ensuite. Il est généralement avancé que la mise sur pied d'un système de T.E.F. suppose des investissements importants qui justifient des accords en vue d'un partage des coûts et des économies d'échelle.

Raisons commerciales, enfin. Les contrats sont des contrats d'adhésion. Bien souvent, la coopération bancaire s'accompagne d'une uniformisation des conditions générales et, d'un alignement du prix des services, du moins en ce qui concerne l'utilisateur. L'uniformisation des contrats résulte notamment de la normalisation technique (Ex. type d'opération pouvant être effectuées ...). Celle-ci justifie que des accords sur la normalisation des contrats soient conclus, du moins s'agissant des clauses relatives aux aspects techniques. Il est en effet inconcevable que les clients puissent négocier le contrat sur ce plan, sans quoi le système serait non opérationnel[1].

Des accords entre banques existent. On songe par exemple à l'accord entre Bancontact et Mister Cash en Belgique, au protocole d'accord carte Bancaire en France, à l'accord notifié par l'association des banques italiennes (A.B.I.). L'accord français du 31 juillet 1984 a pour but de rendre compatibles les automates de retrait et de paiement, d'établir une politique tarifaire commune, notamment s'agissant la commission "d'interchange", c'est-à-dire la commission versée par la banque du bénéficiaire à celle du donneur d'ordre et des coûts mis à charge du porteur de la carte bancaire (les tarifs sont fixés en fonction du type de carte. Ainsi par exemple, les taris peuvent être différents, suivant qu'on demande une carte de paiement nationale ou internationale.
L'accord laisse une liberté, s'agissant de la fixation des tarifs avec les commerçants et la politique commerciale des émetteurs de cartes (forme et emplacement du logo, prestations complémentaires).

2. La décision Eurochèque

La décision de la Commission des Communautés Européennes du 10 décembre 1984 relative aux accords concernant les Eurochèques uniformes [2], mérite d'être examinée dans la mesure où les accords visés ressemblent à ceux qui peuvent être conclus à propos des systèmes de T.E.F. La

Commission a accordé une exemption d'interdiction, estimant que les conditions de l'article 85-§3 étaient réunies.

L'article 85-§3 exige pour son application la présence cumulative de 4 conditions:

1) que la pratique concertée contribue à améliorer la production ou la distribution des produits ou à promouvoir le progrès technique ou économique;

2) que les utilisateurs en retirent un profit équitable;

3) que les restrictions de concurrence soient indispensables;

4) que le champ de restriction de la concurrence soit limité.

Quant à la première condition , la Commission déclare que les accords conclus dans le cadre des Eurochèques contribuent à améliorer les facilités de paiement à l'intérieur du marché commun notamment parce que les chèques peuvent être tirés et encaissés auprès de banques établies dans divers pays étrangers et qu'ils peuvent être tirés en monnaie locale.

La Commission admet les restrictions indispensables au bon fonctionnement du système eurochèque car, bien que la Commission ne le dise pas dans ces termes, ce qui permet le système, c'est le réseau des banques participantes. De plus, si les commissions étaient négociées de façon bilatérale, de banque à banque, une compensation centralisée serait impossible et les frais de traitement augmentés. La Commission argue enfin que si le montant maximal garanti n'était pas uniforme, le système serait impraticable (vérification de l'accepteur du chèque au cas par cas) et inutilement compliqué .

Enfin, concernant les possibilités de concurrence, la Commission constate que le choix s'offre aux utilisateurs entre différents moyens de paiement et que les accords ne régissent pas les relations entre les banques tirées et les clients, une "possibilité de concurrence subsiste au niveau des relations entre chaque établissement émetteur et sa clientèle".

La Commission conclut que son appréciation ne vaut que pour autant que

les accords et décisions en cause ne soient pas complétés au plan national par des accords portant sur les commissions, que "la liberté de choix de l'usager serait illusoire si tous les établissements de crédit d'un même pays offraient le même service au même prix".

3. Application aux T.E.F.

Pour reprendre des éléments similaires à ceux identifiés par la Commission dans la décision Eurochèque, on dira que les accords que suppose la mise sur pied d'un système de T.E.F. international, permettraient le paiement à l'étranger auprès des commerçants de ce pays, et le retrait de monnaie locale.
Ils contribueraient donc à améliorer les facilités de paiement à l'intérieur du Marché Commun et favoriseraient donc le commerce entre Etats membres par une distribution des produits plus aisée.

Des accords de coopération peuvent stimuler le progrès technique pouvant à son tour favoriser la concurrence entre Etats membres (par exemple, des accords concernant la carte à mémoire).

Le profit retiré par les utilisateurs devrait, d'après les critères dégagés par la Commission, être considéré comme équitable. En effet, un réseau européen devrait permettre aux utilisateurs de disposer de toutes les monnaies européennes et ce, en fonction de leurs besoins. Certains systèmes accordent un délai pendant lequel aucun intérêt débiteur n'est dû. Un accord portant sur un tel système au niveau international devrait normalement procurer cet avantage également. Enfin, un réseau européen des T.E.F. présenterait des avantages accessoires tels que l'accès au service et par là l'acquisition de biens après les heures d'ouverture des agences bancaires et de certains commerces (ex. : stations - service), la diminution des risques attachés au transport de fonds ou de chèques, et éventuellement des services accessoires de comptabilité domestique.

Les restrictions qui résulteraient d'accords sur les T.E.F. revêteraient-elles un caractère indispensable? L'argument tiré de l'organisation d'un réseau d'institutions financières est évidemment défendable s'agissant des T.E.F.. L'accent peut aussi être mis sur le fait que la diversité des systèmes nuit à leur utilisation et en réduit l'intérêt pratique pour le consommateur.

C'est au niveau de l'affectation possible de la concurrence que les inquiétudes sont les plus légitimes. Si elles sont moins fondées s'agissant de la concurrence entre différents moyens de paiement, elles le sont davantage quant aux relations entre les établissements financiers et leurs clients. La Commission a eu l'occasion de se prononcer sur les accords notifiés récemment par l'A.B.I., notamment sur la convention interbancaire Bancomat [3].

Cet accord portait notamment sur les conditions de gestion du service, les commissions pour chaque opération et leur répartition entre la banque payeuse et la banque émettrice, la répartition des coûts de gestion entre les banques participant à l'accord et les conditions générales proposées aux utilisateurs.
La Commission s'est proposée de prendre une décision d'attestation négative à l'égard de cet accord.

Notes du point X

[1]Les clauses dont l'uniformité s'explique sur le plan technique, sont les clauses les moins "sensibles" du point de vue du consommateur.

[2] J.O.C.E., 7 février 1985, L. 35/43.
Le profit retiré par les utilisateurs apparaît aux yeux de la Commission équitable dans la mesure où les porteurs de chèques disposent de toutes les monnaies européennes, qu'ils peuvent retirer de l'argent en fonction de leurs besoins sur place, qu'ils bénéficient d'un certain crédit non assorti d'intérêts débiteurs et que le taux de change leur est plus avantageux.

[3] J.O.C.E., 8 octobre 1986, C 251/2 ; cfr. aussi la position de la Commission telle qu'exprimée par Lord Cockfield en réponse à une question parlementaire de M. Abelin relative à la compatibilité de l'entente entre les banques françaises avec les règles du droit communautaire (Question écrite n° 7/85, J.O.C.E., C 251/10 du 2 octobre 1985) ; cfr. également la question de Madame Van Hemeldonck concernant la compatibilité de l'accord entre les banques belges au regard de l'article 85 du Traité (Question écrite n° 970/85, J.O.C.E., C 310/10 du 2 décembre 1985) ; cfr. enfin la communication de la Commission au Conseil COM (86) 754 final "Tout atout pour l'Europe : les nouvelles cartes de paiement", n° 17.

XI. ACTIONS EUROPEENNES

Les actions européennes se situent à quatre niveaux

1. Un texte de réflexion de la DG XV sur les cartes de paiement

(COM (86) 754 final)

1) Le critère d'application du texte est un critère technique : seules sont visées les cartes munies de pistes magnétiques et/ou de micro-processeurs. Cette approche fondée sur les cartes rappelle celle de la loi danoise encore qu'elle soit plus restrictive au niveau du support.

Seules sont visées les cartes tendant à réaliser certaines opérations de "paiement électronique" essentiellement retrait de billets et paiement). Ne sont par exemple pas visées les cartes permettant d'obtenir des informations sur un compte (telles que par exemple la carte TELES).

Ressortent du rapport (annexe), la multiplicité des cartes classifiées d'après leur fonction et la difficulté d'établir une unification terminologique vu le caractère multifonctionnel de nombreuses cartes et la diversité de leurs sources d'émission (banque, secteur pétrolier, grande distribution).

2) Le rapport se situe dans l'optique de l'achèvement du marché intérieur européen. Les nouveaux moyens de paiement sont perçus comme devant faciliter le commerce intra-communautaire. Comme, une distorsion dans leur régime dans les différents Etats membres pourrait exercer l'effet inverse, une intégration financière prenant en compte un nouveau moyen de paiement apparaît nécessaire (notamment l'application de l'article 106 du Traité consacrant le principe de la liberté des paiements). Enfin, cette action s'inscrit dans le cadre de la politique de la technologie ; l'avance technologique acquise par l'Europe dans le domaine des cartes de paiement (Ex : cartes à micro-processeurs) devrait permettre l'ouverture de vastes marchés extérieurs pourvu que ce savoir-faire soit valorisé par une politique d'accompagnement bien pensée. L'initiative de la Commission se propose d'accompagner les efforts d'ouverture nécessaires par des mesures destinées à aider des organismes concernés à réaliser

l'interopérabilité des systèmes mis en place (n° 5). Le cadre de référence proposé s'articule autour de trois principes :

1. le principe de réciprocité visant à ouvrir mutuellement les différents systèmes. Ce principe, déjà largement mis en œuvre s'agissant des distributeurs doit être plus largement aménagé s'agissant des terminaux points de vente. Un code de bonne conduite préparé par la Commission devrait servir de guide (cfr. infra) ;
2. la normalisation et l'interconnexion des réseaux qu'implique l'ouverture des systèmes à l'échelle européenne ne devrait porter atteinte à la libre concurrence ;
3. l'équilibre entre la sécurité technique des systèmes et le coût de celle-ci.

Outre ces aspects principaux, la Commission évoque une série d'aspects réglementaires complémentaires tels la surveillance des institutions émettant des cartes et/ou gérant des systèmes de cartes, la protection des données, le problème de la TVA, les questions liées aux relations contractuelles (notamment la protection des consommateurs ; cfr. infra B. le projet de réglementation de la DGXI).

2. Des projets de réglementation concernant l'émission et l'utilisation des cartes.

2.1. Un avant-projet de texte sur l'utilisation des cartes (DG XI/B)

Nous nous limitons à quelques remarques générales sur le projet :

1) quant à son principe : est-il opportun, à ce stade du développement technologique, de figer celui-ci en se focalisant sur les cartes et non sur le transfert électronique de fonds, quel qu'en soit le mode d'initiation ? Le terme carte est trop étroit. Il serait indiqué de le remplacer par "moyens d'accès" comme le fait par exemple la loi américaine.

2) quant à son contenu : le projet ne contient aucune définition de son champ d'application. A notre avis, deux types d'approches sont possibles :

- une approche qui lie le champ d'application du projet à la notion de carte.

Il y aurait lieu alors de préciser le type de cartes visé ou les opérations aux fins desquelles la carte est utilisée. On peut supposer à la lecture du projet que seules sont visées les cartes dont l'utilisation ne s'accompagne pas de la production d'un écrit signé.

- une approche centrée sur la notion de transfert électronique de fonds défini largement (sur les problèmes posés par une telle définition voir supra point II)

Plus fondamentalement, ne faudrait-il pas s'interroger sur l'opportunité d'une directive beaucoup plus générale qui traiterait non pas des problèmes juridiques liés à telle catégorie d'opérations ou à tel type de moyens d'accès mais bien de la façon de résoudre les questions essentielles soulevées en droit par la "dématérialisation" [1] des transactions et l'interposition de la machine entre les parties.

Dans le même ordre d'idées, on constate que le projet de directive aborde des problèmes classiques ayant trait à l'information de l'utilisateur sur les conditions du service, ou l'imposition de certaines règles (relatives à la responsabilité notamment) auxquelles il ne semble pas permis de déroger.
Ne faudrait-il pas laisser à des directives plus générales le soin de régir des problèmes qui relèvent de la politique de protection du consommateur (information et clauses abusives).

L'article 11 traite un problème classique du droit bancaire, l'irrévocabilité des ordres de paiement qui devrait être réglée dans une directive rapprochant les législations bancaires.
Il est curieux de constater que cet article 11 entérine un souhait des commerçants et des banques mais va à l'encontre des lois récentes, française notamment sur l'information et la protection du consommateur (voir considérations supra)

3) Le problème de la preuve, crucial et le seul qui, d'ailleurs soit vraiment spécifique aux transactions télématiques est, quant à lui, traité de façon très succincte dans l'article 1°.

Cet article semble ambigu et pêche par manque de précision. Si le ticket est un élément de preuve parmi d'autres pouvant tenir lieu de présomption,

il y va là d'une application classique des principes qui ne doit pas être répétée. Si par contre il s'agit d'affirmer que le ticket produit constitue pour l'institution financière en cas de retrait ou l'utilisateur en cas de dépôt un mode de preuve suffisant, on se trouve alors devant une dérogation difficilement justifiable à un principe fondamental de notre droit de la preuve suivant lequel les documents probatoires doivent être constitués contradictoirement. D'autres dispositions du texte (Art. 6 §§ 1,2,3 ; Art. 8 §§1,2,3 ; Art. 9 ; Art. 12 §§ 1,2 ; Art. 13 et 14) contribuent à alimenter le problème de la preuve : comment prouver le moment où l'utilisateur constate la perte de sa carte (Art. 6), comment établir la défectuosité du système (Art. 8), ...

4) Les problèmes liés à la multiplicité des intervenants dans les transferts électroniques de fonds (Art. 12 à 14 du projet) gagneraient à être approfondis.

2.2. Un projet de recommandation de la Commission portant sur un Code européen de bonne conduite en matière de paiement électronique (DG III/2357/86/Rev. 2)

Ce projet, en voie de modification, au moment où est rédigée la présente étude, ne sera pas examiné en détail.
Certaines des remarques formulées plus haut peuvent également trouver à s'appliquer : ainsi, la définition du paiement électronique relativement restrictive s'appuyant sur la notion de carte à piste magnétique ou à micro-processeur, l'irrévocabilité de l'ordre de paiement (mais cette question est sans doute théorique étant donné que l'autorisation rend en pratique la révocation malaisée), l'imputation des responsabilités pour mauvais fonctionnement de l'appareil (dans quelle mesure les règles classiques relatives à la responsabilité du fait des choses dont le critère est la garde ne sont-elles pas adéquates ?).

3. Des actions normatives concernant indirectement les transferts électroniques de fonds

1. Directive du 28 mars 1983 prévoyant une procédure d'information dans

le domaine des normes et réglementations techniques (J.O.C.E., L 109/8 du 26 avril 1983).

2. Directive du 24 juillet 1986 concernant la première étape de reconnaissance mutuelle des agréments d'équipements terminaux de télécommunications, J.O.C.E., L 217/21 du 5 août 1986).

3. Recommandation du Conseil du 22 décembre 1986 concernant l'introduction coordonnée du réseau numérique à intégration des services (RNIS) dans la Communauté européenne (J.O.C.E. du 31 décembre 1986, L. 382/36[2]).

4. Décision du Conseil du 22 décembre 1986 concernant la standardisation de la technologie de l'information et des télécommunications (J.O.C.E., 1987, L. 36/31).

4. Des études et recherches concernant directement ou indirectement les transferts électroniques de fonds :

1. **Des études techniques** concernant indirectement les transferts électroniques de fonds :

A. Programme COST (coopération en sciences et technologies) contribuant notamment au financement du projet OSIS (Open Shop for Information Systems) lequel vise à développer un système technique constituant l'usage d'une carte programmable avec celui d'un code mathématique pour assurer l'intégrité du message et l'identification des parties communiquant [3]. Ce système devrait réaliser un équilibre entre l'ouverture des systèmes et la sécurité. Le système OSIS se présente comme l'équivalent fonctionnel de la signature et présente un intérêt non seulement pour les transferts électroniques de fonds mais également pour la conclusion de contrats par télématique. Ce système essentiellement technique devrait avoir des répercussions au niveau juridique dans la mesure où la fiabilité des moyens de télécommunications est appelée à croître limitant les problèmes de preuve, de fraudes et d'atteintes à la vie privée.

B. Programme ESPRIT (European Strategic Program for Research and

Development in Information Technologies).

C. Programme RACE

D. Programme TEDIS ("Proposition de réglement du Conseil instaurant la phase préparatoire d'un programme communautaire relatif au transfert électronique de données à usage commercial utilisant les réseaux de communication : COM (86) 662 final).

E. Programme STAR ("Règlement n° 3300/86 du Conseil du 27 octobre 1986 instituant un programme relatif au développement de certaines régions défavorisées de la Communauté par un meilleur accès aux services avancés de télécommunications, J.O.C.E., L. 305/1 du 31 octobre 1986).

2. Des études d'impact : Programme FAST(Forecasting Assessment Science and Technology).

3. Des études juridiques : projet Legal Observatory (DG XIII). Le but de ce projet est de réunir périodiquement des experts des différents Etats membres afin de débattre des problèmes juridiques relatifs au développement d'un marché européen de l'information et des éventuelles solutions à apporter.

Des recherches sont également confiées à des centres de recherches. On notera une étude menée conjointement par le C.R.I.D. (Namur), le GMD (Bonn), Le Legal Technology Group (Londres) et le Computer/Law Institute (Amsterdam) dont un des thèmes concerne les transferts électroniques de fonds à vocation "grand public".

Notes du point XI

[1] Dématérialisation est un terme quelque peu elliptique dans la mesure où les nouvelles technologies de traitement et de transmission de l'information n'aboutissent pas à la disparition complète des supports. La question demeure cependant de savoir si ces supports, vu leurs conditions de production, répondent aux exigences juridiquement requises.

[2] Cfr. l'avis du Comité Economique et Social, J.O.C.E. du 22 décembre 1986, C 328/10).

[3] Pour un aperçu d'OSIS, voyez H. BURKERT, "Une expérience positive de solution juridico-technique : le projet OSIS", Les transactions internationales assistées par ordinateur", LITEC, Paris, 1987, pp. 139-152.

LE TRANSFERT ELECTRONIQUE DE FONDS DANS SES APPLICATIONS GRAND PUBLIC : PROBLEMES JURIDIQUES GENERAUX

PLAN DE L'ETUDE