Dématérialisation, authentification et responsabilité

Amory, Bernard; Thunis, Xavier

Published in:
Les transactions internationales assistées par ordinateur

Publication date:
1987

Document Version
le PDF de l'éditeur

Seconde Partie

LA REGULATION JURIDIQUE DES TRANSACTIONS INTERNATIONALES ASSISTEES PAR ORDINATEUR

CHAPITRE I

DEMATERIALISATION, AUTHENTIFICATION

ET RESPONSABILITE

Bernard Amory

Assitant au Centre de Recherches Informatique et Droit des Facultés universitaires de Namur, Associate in the Law Offices of Dechert Price & Rhoads (Bruxelles), Belgique.

Xavier Thunis

Assistant au Centre de Recherches Informatique et Droit des Facultés universitaires de Namur, Belgique.

SOUS-CHAPITRE I

LE DROIT CONTINENTAL

L'objet de cette étude sur l'authentification (de l'origine et du contenu) des transactions sans papier et sur les questions de responsabilité que celles-ci soulèvent (cf. l'intitulé du chapitre), paraîtra sans doute moins obscur si d'emblée nous en définissons les concepts essentiels, délimitant par la même occasion l'objet de nos recherches.

Quand une convention est passée entre plusieurs personnes, une série de litiges peuvent surgir : il arrive que les parties contractantes ou les tiers, de façon très radicale, mettent en cause *l'existence* même du contrat et, le principe même de celui-ci étant contesté, il appartient à la partie qui s'en prévaut de montrer qu'il a été conclu. On peut rattacher à cette hypothèse la contestation relative à l'identité des parties contractantes, l'une d'entre elles niant avoir jamais conclu une convention génératrice d'obligations dont l'autre entend se prévaloir.

Moins fondamentalement, certaines dispositions de la convention conclue peuvent être contestées, ce qui déplace l'interrogation sur le contenu de celle-ci.

Deux grandes questions se posent donc lors de la passation d'un contrat : *qui contracte* et *sur quoi* porte l'accord, cette seconde question ne nous référant pas seulement à l'interprétation de clauses acceptées, mais aussi à la détermination même du « champ contractuel ».

Ces deux questions, *origine et contenu des conventions* ne sont pas neuves et, en 1804, les auteurs du Code Napoléon y ont cherché et donné réponse en affirmant la prééminence de la preuve écrite des actes juridiques, la signature permettant, en principe, de rapporter l'acte à celui qui l'a posé. Sans prétendre que les progrès techniques de l'audio-visuel, des télécommunications et de l'informatique, d'autant plus importants que joue leur synergie, amèneront inéluctablement une disparition de l'écrit ou du papier, leur influence se fait et se fera sentir dans le monde des juristes qu'elle oblige à repenser leurs catégories, voire à en créer de nouvelles.

Ainsi, la combinaison des technologies de l'informatique et des télécommunications appelée télématique permet le traitement et la transmission des données à distance.

Que l'on songe aux banques de données juridiques ou scientifiques dont le contenu peut être mobilisé par un utilisateur établi à plusieurs milliers de kilomètres, à la transmission de données financières dans un réseau tel que S.W.I.F.T. (1) aux transferts électroniques de fonds ou, de façon plus générale, aux « contrats à distance » dont la télématique favorise la conclusion ou l'exécution.

Par-delà la diversité des applications citées, le juriste est surtout sensible à la « *dématérialisation* » *des transactions* passées. Cette dématérialisation est double : d'une part, l'objet de la transmission, l'information, est toujours immatériel, seul le mode de transmission de cette information pouvant revêtir un caractère matériel (exemple : transmissions d'informations sur support papier),

d'autre part, ce transfert même tend à s'opérer sans fixation durable et quasiment sans incorporation de l'information à un support papier, voire même à un quelconque support matériel.

Ces deux pôles de la dématérialisation ne sont certes pas neufs : les contrats de transfert d'information existent sans doute depuis qu'existe une inégalité dans l'accès à l'information et le téléphone permet depuis longtemps déjà la conclusion de contrats à distance.

Mais par la rapidité qu'elle imprime à la circulation de l'information

(1) Society for Worldwide Interbank Financial Telecommunications.

et par la multiplication des possibilités de conclure ou d'exécuter à distance sans support durable, sinon tangible, la télématique multiplie et réactive des problèmes de preuve jusque là marginaux.

Inutile de souligner la difficulté d'appliquer un droit de la preuve vénérable à une technique en pleine évolution.

La première partie de notre exposé sera consacrée à l'examen et à la solution de ces difficultés de preuve, avec une attention particulière aux problèmes d'authentification (2) des actes ne portant pas de signature manuscrite.

Dans une seconde partie, nous examinerons les questions de responsabilité liées aux « transactions sans papier » (3) et plus précisément, aux transactions financières (section II).

Nous verrons que le grand nombre de parties impliquées dans une opération télématique rend difficile l'identification de la cause d'un dommage et que, par ailleurs, la complexité technologique d'une opération de ce genre peut amener à poser les problèmes de responsabilité en terme de risque.

Notons enfin que la liaison des questions de preuve et de responsabilité dans un même exposé n'est pas fortuite, l'attribution de la charge de la preuve et la détermination des modes de preuve admissibles réagissant sur le fond du droit.

Dernière précision : le concept de « droit continental » est entendu ici de façon particulièrement restrictive puisque l'analyse juridique se fera à la lumière des grands principes du droit privé, français et belge.

(2) Sur le concept d'authentification, D. Syx, Naar nieuwe vormen van handtekening in het elektronisch geld verkeer, Kredietbank, 30 augustus 1985 n° 10.
(3) Nous préciserons ce concept dans la suite de l'exposé.

SECTION I

AUTHENTIFICATION DES TRANSACTIONS COMMERCIALES ASSISTEES PAR ORDINATEUR

Les opérations (4) d'une entreprise peuvent être regroupées en deux catégories (5) :

— *les opérations interentreprises* telles que les contrats, les ordres ou les confirmations de commande, les ordres de paiement, etc... que nous désignerons plus généralement par les termes : « Transactions commerciales »,

— *les opérations intraentreprises* matérialisées par des documents tels que les inventaires, les documents destinés à répondre aux exigences de la législation comptable, fiscale, douanière, etc...

Seule la première catégorie retiendra notre attention dans la présente étude.

Le document « papier » a été longtemps, et est encore le plus souvent, utilisé pour « enregistrer » tant des opérations interentreprises qu'intra-entreprises. Ses avantages sont connus : transmission aisée, durée de conservation relativement longue, falsification difficile et, en tout cas, détectable. Grâce à ces qualités, le document papier sert de support de données et assure une fonction *d'information*. A condition de remplir certaines exigences, il peut aussi faire *preuve* des données qui y sont portées.

En outre, certains documents papier ont la particularité d'incorporer les droits qui s'y attachent de telle sorte qu'ils représentent ces droits. Le document a alors une fonction symbolique (6). Le connaissement, la lettre de change, le crédit documentaire sont des exemples types de documents ayant une fonction symbolique.

L'authentification ressortit à la fonction probatoire. Elle revêt

(4) Nous n'utiliserons pas, dans le texte, l'expression « transaction sans papier », qui nous paraît peu adaptée puisque l'emploi conjugué de l'informatique et des télécommunications aboutit rarement à une disparition totale du papier. La question fondamentale est, en fait, la suivante : le papier ainsi produit est-il un écrit auquel le droit (continental) reconnaît une force probante ?
(5) Sur la distinction, voir Legal value of computer records, United Nations commission on international trade law A/CN9.265 p. 4.
(6) Pour plus de détails, voir Aspects juridiques de l'échange automatique de données commerciales, Nations-Unies, Conseil Economique et Social TRADE/WP4/R. 185/Rev. 1er octobre 1982, p. 8 et s. et p. 22 et s.

elle-même deux fonctions complémentaires : identifier la personne qui en est l'auteur et indiquer sa volonté de s'approprier le contenu du message ou du document (7). Comme le souligne la Commission des Nations Unies pour le droit commercial international, « en cas de différend, l'authentification constitue sur ces points un élément de preuve » (8).

L'authentification pourra donc servir à rapporter la preuve d'une transaction commerciale c'est-à-dire démontrer vis-à-vis des personnes qui y sont parties et des tiers que celle-ci a bien eu lieu entre ces parties et quel en est le contenu.

Depuis que l'écriture n'est plus l'apanage d'une élite, l'authentification est traditionnellement assurée par la signature manuscrite, éventuellement combinée avec l'intervention d'un notaire ou autre officier public (9). Toutefois, comme le souligne la C.N.U.D.C.I. dans le document précité, « les exigences du commerce moderne ont conduit de nombreux systèmes juridiques à autoriser une signature apposée au moyen d'un cachet, d'un symbole, d'un fac-similé, de perforations ou de tout autre procédé mécanique ou électrique... »

Ainsi, en droit français, la loi n° 66-380 du 16 juin 1966 « relative à l'emploi de procédés mécaniques pour apposer certaines signatures sur les effets de commerce et le chèque » a partiellement entériné la pratique de signer certains effets de commerce au moyen d'une griffe ou d'un fac-similé (10).

En droit belge, certaines dispositions légales autorisent exceptionnellement l'emploi de la griffe (par exemple pour la signature par les administrateurs des actions et obligations de sociétés et pour la signature des billets de la Banque Nationale). Il existe également certaines pratiques qui font fi de la signature manuscrite. Tel est le cas des contrats d'assurances signés par la compagnie d'assurances au moyen d'une griffe ou d'une signature imprimée ou cachetée. De telles pratiques seraient *contra legem* (11).

Enfin, en droit international, certaines conventions contiennent des dispositions autorisant l'usage de procédés électroniques à titre de signature du moins lorsque ceux-ci ne sont pas incompatibles avec le

(7) Telles sont les fonctions attribuées par M. Van Quickenborne à la signature qui, ainsi que nous le voyons ci-après, est une forme d'authentification. Voir M. Van Quickenborne, Quelques réflexions sur la «signature des actes sous seing privé. Note sous Cass., 28 juin 1982, R.C.J.B., 1985, p. 57 à 104.
(8) C.N.U.D.C.I., Doc. A/CN 9/265 du 21 février 1985, p. 16.
(9) Avant la généralisation de l'écriture, l'authentification était assurée par un sceau ou seing (voir H. de Page, Traité élémentaire de droit civil belge, Bruxelles, 1967, tome III, n° 777).
(10) M. Van Quickenborne, op. cit.
(11) H. De Page, op. cit., n° 778 et 778 bis.

droit national du pays concerné (12).

Les procédés évoqués ci-dessus qui ont été admis à remplacer dans certains cas la signature manuscrite sont inapplicables aux transactions télématiques, c'est-à-dire réalisées grâce à l'intervention conjointe d'ordinateurs et des télécommunications. La griffe ou le cachet ne peuvent être apposés à distance. Ils nécessitent la présence physique de leur titulaire. La télématique requiert donc de nouvelles techniques d'authentification adaptées à ses caractéristiques propres, essentiellement la possibilité de réaliser des opérations à distance et en temps réel (13). Diverses techniques d'authentification adaptées à la télématique ont déjà été élaborées, d'autres sont sur le point de l'être.

Sans vouloir être exhaustifs dans l'énumération de ces techniques, ni détaillés dans leur description, nous en donnons un aperçu dans la section 2. Dans le point 3, nous examinerons quelles sont les exigences légales du droit français et belge et la pratique des affaires en matière d'authentification dans ces pays. Préalablement, afin d'essayer de concrétiser la problématique, nous décrirons dans le point 1 une opération internationale de transfert électronique de fonds à titre d'illustration en soulignant les points où une authentification est nécessaire.

Tout au long de ce chapitre, nous nous attacherons à, d'une part, souligner les implications de la dématérialisation de l'authentification inhérente au traitement et à la transmission par des moyens automatisés et, d'autre part, à en examiner l'incidence sur la force probante (« la foi » selon les termes du Code Civil) qu'on peut attacher aux transactions commerciales dématérialisées tant en ce qui concerne leur contenu que leur origine. Par contre nous n'examinerons pas les implications de la dématérialisation sur les fonctions symbolique et purement informative évoquées ci-dessus.

(12) A titre d'exemples, on citera l'article 14(3) de la United Nations Convention on the carriage of goods by sea (Hamburg 1978) et l'article 5(1) de la Convention on Freight Agreements in International Road carriage nf goods. De même, lors des discussions préparatoires à la Convention de Genève sur le chèque, il a été souligné que le mot « signature » désigne tout signe matériel quelconque servant, selon les usages du pays, à identifier sur des papiers ou effets la personnalité de celui qui l'appose (rapporté par M. Vasseur et C. Marnl, Le chèque, Sirey, Paris, 1969, p. 100).

(13) Pour plus de détails sur la télématique et ses différents aspects, on consultera utilement : La télématique, aspects techniques, juridiques et socio-politiques, t. 1 et 2, Actes du Colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur, éd. Story-Scientia, Gand, 1984-1985.

1. — UNE ILLUSTRATION INTERESSANTE : L'AUTHENTIFICATION DANS UN TRANSFERT ELECTRONIQUE DE FONDS INTERNATIONAL

Le secteur bancaire est l'un des premiers à s'être automatisé et informatisé. Actuellement, la plupart des entreprises des autres secteurs sont également informatisés. Grâce à la possibilité de relier par télécommunication les ordinateurs respectifs des banques et de leurs clients, une entreprise peut aujourd'hui effectuer un paiement au profit d'un de ses partenaires sans qu'il soit fait usage du moindre écrit traditionnel, du déclenchement de l'opération jusqu'à son aboutissement. Une telle opération de transfert électronique de fonds (14) donne d'excellents exemples d'authentification. Le schéma ci-après décrit une opération internationale de transfert électronique de fonds en faisant apparaître les différents points d'authentification.

Dans l'opération représentée, une entreprise située à Bruxelles (entreprise A, donneuse d'ordre) effectue un paiement au profit de son fournisseur à Paris (entreprise B, bénéficiaire). L'opération est complètement dématérialisée : elle s'effectue sans écrit traditionnel.

L'entreprise donneuse d'ordre et l'entreprise bénéficiaire sont reliées à leurs banques respectives par un système de gestion électronique de leurs comptes à distance. Ce système permet à l'entreprise A de donner un ordre de paiement à sa banque A via leurs ordinateurs respectifs reliés par télécommunication sans aucun support papier. L'entreprise B, bénéficiant du même service de la part de sa banque C pourra consulter son compte à distance sur son terminal relié par télécommunication à l'ordinateur de la banque C et donc vérifier si le montant du paiement effectué par l'entreprise A lui a été crédité.

Les banques intervenantes étant membres du réseau de télétransmisson interbancaire international S.W.I.F.T. (Society for Worlwide Interbank Financial Telecommunications), le transport du message (l'ordre de paiement) sera confié à ce réseau et s'effectuera selon les normes et procédures (notamment d'authentification) qui lui sont propres. Les banques A et B étant en relation bancaire directe, le règlement de l'opération se dénouera entre elles par débit du compte de la banque A auprès de la banque B.

Si le bénéficiaire (entreprise B) a un compte auprès de la banque B, celle-ci pourra dénouer l'opération en créditant le compte de l'entre-

(14) D'un point de vue juridique, le transfert électronique de fonds défini par D. Sys comme étant « tout transfert de fonds engendré non pas par un instrument de papier mais uniquement par des moyens électroniques ou télématiques », D. Sys, Aspects juridiques du mouvement électronique de fonds, Kredietbank, Bruxelles, 1982, p. 12-13.

prise B. De même, si le bénéficiaire n'a pas de compte auprès de la banque B mais en dispose d'un auprès d'une autre banque qui est en relation de compte avec la banque B, l'opération de compte pourra être dénouée entre ces deux institutions via leurs propres moyens de communication.

Par contre, si comme dans l'exemple illustré ci-après le bénéficiaire est domicilié auprès d'une banque C avec laquelle la banque A n'est pas directement en relation de compte, le règlement de l'opération se fera via un réseau et une chambre de compensation dont les deux banques (B et C) sont membres.

Dans notre exemple, les banques B et C étant situées en France, il y aura un mouvement aux comptes dont elles sont obligatoirement titulaires auprès de la Banque de France. Ce mouvement pourra être déclenché et opéré de façon tout à fait dématérialisé via le système S.A.G.I.T.T.A.I.R.E. (Système Automatique de Gestion Intégrée par Télétransmission de Transactions avec Imputation de Règlements «Etranger») et le C.C.M.B. (Centre de Commutation des Messages Bancaires) (15). La banque B qui a reçu via S.W.I.F.T. l'ordre de payer le bénéficiaire domicilié auprès de la banque C va adresser à la Banque de France par télétransmission l'ordre de débiter son compte en créditant le compte dont dispose la banque C auprès de cette même institution. Ensuite, la Banque de France avertira la banque C de ce crédit. La banque C le portera alors au compte du bénéficiaire lequel pourra en être immédiatement informé par la consultation à distance de l'état de ses comptes (16).

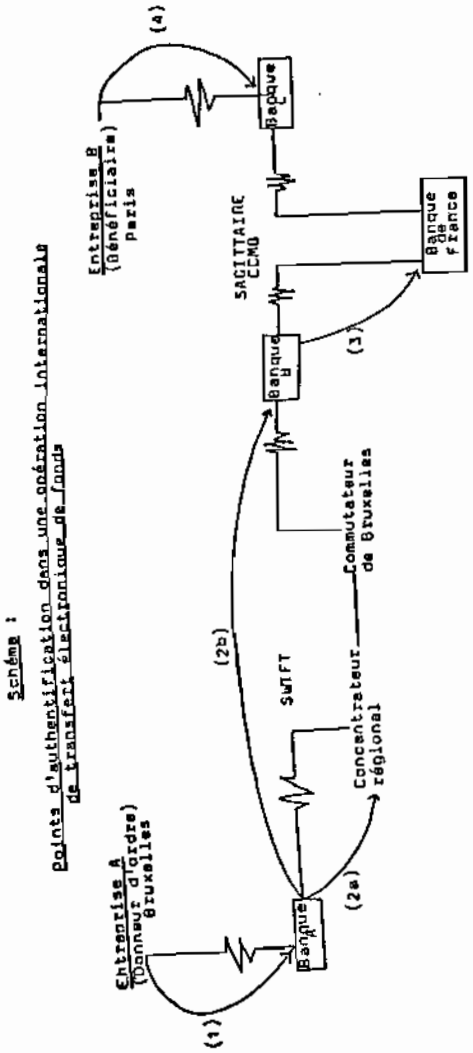
Dans l'opération particulièrement complexe décrite ci-dessus, apparaissent quatre points d'authentification :

1. L'entreprise A, donneuse d'ordre, devra s'authentifier vis-à-vis de sa banque A selon la procédure convenue entre elles, afin que cette dernière soit assurée qu'elle est autorisée à débiter le compte de l'entreprise A ;

2. Pour transmettre le message à la banque B via le réseau S.W.I.F.T., il appartiendra à la banque A de s'authentifier

(15) Pour une description des systèmes S.A.G.I.T.T.A.I.R.E. et C.C.M.B., voir Banque de France, Service de l'information, Note d'information n° 63, novembre 1984

(16) On notera que si la banque C n'offre pas à son client, l'entreprise B, un système de gestion télématique de ses comptes, l'entreprise B pourra néanmoins consulter son compte auprès de sa banque C par voie télématique si elle bénéficie d'un service de gestion télématique de ses comptes auprès d'une autre banque (banque D) qui, ayant passé un accord avec la banque C, reçoit les informations relatives aux comptes du client commun auprès de la banque C et les transmet par télématique au nom de la banque C à l'entreprise B.



selon les procédures prévues par ce système, c'est-à-dire vis-à-vis du destinataire, la banque B ;

3. Pour transmettre le message à la banque C et opérer le règlement de l'opération via le système S.A.G.I.T.T.A.I.R.E. - C.C.M.B., la banque devra s'authentifier auprès de la Banque de France selon les procédures prévues par ce système ;

4. Enfin, pour consulter l'état de son compte auprès de sa banque C, l'entreprise B, bénéficiaire du paiement, devra s'authentifier auprès de cette banque selon la procédure convenue entre elles.

II. — LES TECHNIQUES MODERNES D'AUTHENTIFICATION

Il existe trois grandes catégories de techniques modernes d'authentification : le mot (ou nombre) de passe (souvent combiné avec une carte magnétique) appelé aussi « code secret », la cryptographie et la reconnaissance de caractéristiques physiques (17).

Ci-après figure une brève description de ces techniques et des exemples d'application de celles-ci déjà mis en œuvre dans la pratique des affaires.

D'un point de vue général, on remarquera avec Schwab et d'Alençon (18) que sur le plan pratique, authentification signifie, dans la plupart des cas, vérification : « Un automate compare une information saisie à une référence et décide, selon certaines règles, que l'écart entre les deux est suffisamment petit pour qu'on puisse considérer que la personne est bien celle qu'elle prétend être ».

Ce processus de vérification est également appliqué à la forme traditionnelle d'authentification. En effet, la signature manuscrite fait l'objet par son destinataire soit d'une confrontation à un spécimen de référence (par exemple la vérification de la signature par le préposé de la banque du tireur en cas de présentation d'un chèque au porteur) soit pour des parties en relation d'affaires régulière, d'une confrontation à l'image que s'est faite plus ou moins consciemment chaque partie de la signature habituelle de son partenaire. La vérification peut également se faire selon une procédure spécifiquement prévue par le droit judiciaire. Il s'agit de la procédure de vérification d'écriture.

(17) Vnir D. Syx, Naar nieuwe vormen van handtekening ? Het probleem van de handtekening in het electronisch geld verkeer, op. cit.
(18) T. Schwab et M. d'Alençon, L'authentification des personnes, texte de l'exposé présenté au séminaire international organisé par O.R.O.S. à Paris les 18 et 19 octobre 1984 sur « Les terminaux point de vente - Fraude et sécurité ».

Par rapport à la signature manuscrite, les techniques modernes d'authentification présentent l'avantage de procéder automatiquement à la vérification et ce pour chaque opération. On sait que la vérification de la signature manuscrite n'est qu'occasionnelle.

Il n'en demeure pas moins que même lorsqu'il y a vérification automatique, la plupart des techniques d'authentification ne sont pas infaillibles. Puisqu'elles consistent à vérifier l'importance d'un écart éventuel entre une information saisie et une référence, mais non une égalité entre ces deux facteurs, il y aura toujours, à l'intérieur de cet écart, une marge d'erreur possible. Chaque technique d'authentification devra donc définir son « seuil d'acceptation » en tenant compte que plus ce seuil est bas plus le risque est grand que le véritable titulaire du moyen d'authentification soit refusé par l'automate (taux de vrais refusés élevé). Par contre, plus ce seuil est élevé, plus le risque que des fraudeurs soient acceptés par l'automate est grand (taux de faux acceptés élevé) (19).

L'expérience a déjà prouvé que diverses techniques d'authentification décrites ci-dessus sont au moins aussi et probablement plus fiables que la signature manuscrite.

A. — *LE CODE SECRET.*

L'une des techniques d'authentification (20) les plus répandues est l'authentification par code secret. Celui-ci est constitué d'une combinaison de chiffres (et/ou, éventuellement, de lettres) qui, en principe, est unique et n'est connue que par son titulaire (d'où son appellation anglo-saxonne : « *Personal Identification Number* » - P.I.N.). Le code secret est souvent combiné avec une carte à piste magnétique ou une carte à mémoire. Cela permet une vérification de la validité du code sans que la trace de celui-ci ne reste à la disposition d'un automate contrôlé par un tiers (21).

Le code secret est communément utilisé pour l'authentification dans les transferts électroniques de fonds « grand-public » (opérations aux guichets automatiques de banques et terminaux points de vente) et pour l'accès aux banques de données. Il en est également fait

(19) Voir à se sujet M. Schwab et M. d'Alençon, op. cit.
(20) Cette technique n'assure parfois que la fonction identification de l'authentification et non l'indication de la volonté.
(21) Dans le cas de la carte à mémoire, cela est possible grâce au microprocesseur contenu dans celle-ci. Dans le cas de la carte à piste magnétique, cela est possible grâce à un décodeur qui « compare le code avec celui qu'il calcule selon un algorithme précis, à partir de certaines données stockées sur les pistes de la carte introduite » (D. Syx, Aspects juridiques du mouvement électronique de fonds, KB, Bruxelles 1982, p. 46).

usage dans les systèmes de gestion télématique des comptes bancaires pour entreprises du moins pour les fonctions de pure information (par exemple, consultation des comptes). Les opérations de transfert de fonds ne peuvent être réalisées que moyennant une authentification plus sophistiquée.

Pourtant l'authentification par code secret offre déjà un très haut degré de fiabilité. Ainsi, dans le cas d'un code de quatre chiffres dans un système ne permettant que trois essais, un fraudeur n'a que 0,03 % de chance de découvrir le code secret (22). Toutefois cette technique présente comme inconvénients, un risque élevé de perte ou d'oubli du code par son titulaire et l'accès assuré au fraudeur qui a réussi à se procurer le code.

B. — *LA CRYPTOGRAPHIE*

La cryptographie consiste à coder un texte à l'aide de clés confidentielles et de processus mathématiques complexes (algorithmes) afin de le rendre incompréhensible à toute personne qui en prendrait connaissance sans avoir les moyens de procéder à son déchiffrement, opération symétrique qui rétablit le texte en clair (23).

Comme le rappelle D. Syx (24), on distingue généralement deux grandes catégories de techniques crytographiques : les systèmes symétriques et les systèmes asymétriques.

Dans les systèmes symétriques, l'expéditeur et le destinataire du message disposent de la même clé pour chiffrer puis déchiffrer celui-ci. Ces systèmes ne permettent pas d'assurer les fonctiops de l'authentification étant donné qne chaque partie dispose de la même clé.

Par contre les systèmes de cryptographie asymétrique (aussi appelés systèmes à clés publiques) sont capables d'assurer ces fonctions. Ils fonctionneut sur base d'une double clé (une clé publique et une clé secrète correspondante) qui permet une double opération d'encryptage-décryptage. Ainsi, pour envoyer un message, l'expéditeur cryple d'abord celui-ci au moyen de la clé publique du destinataire (il trouvera celle-ci dans un annuaire ad-hoc). Ensuite, il recrypte le message au moyen de

(22) Voir à ce sujet Ph. Van Heurck, L'authentification dans les systèmes informatiques et télématiques, Actes des Journées Notariales à Tournai les 26 et 27 septembre 1985, Duculot, Gembloux, 1985.

(23) Cette définition est largement inspirée de celle donnée à la p. 9 de la Note d'Information n° 61 de la Banque de France sur S.W.I.F.T. (mars 1984).

(24) D. Syx, Le transfert électronique de fonds. Le droit hésitant face à une réalité galopante, in La Télématique, Actes du Colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur, t. 2, Story Scientia, Gent, 1985, p. 244.

sa propre clé secrète. Le destinataire décrypte alors le message d'abord au moyen de sa clé secrète puis au moyen de la clé publique de l'expéditeur.

Certains systèmes de gestion télématique des comptes bancaires pour entreprises utilisent, du moins pour les opérations délicates comme les ordres de paiement, la cryptographie de type asymétrique (25).

Le réseau S.W.I.F.T. assure la confidentialité par un cryptage symétrique et l'authentification par une procédure d' « habilitation logique » *(« log-in »)*. En vertu de cette procédure, les membres de S.W.I.F.T. disposent d'une « table de *log-in* » (confidentielle, composée de deux parties qui se complètent et sont envoyées par plis séparés et remplacées régulièrement). Pour s'authentifier, la banque émet un message de *log-in* au centre de commutation dont elle dépend. Si les nombres secrets contenus dans le message satisfont au contrôle auprès de S.W.I.F.T., une notification d'habilitation *(« log-in acknowledgement »)* accompagnée d'un autre nombre secret est adressée par S.W.I.F.T. à l'adhérent. Celui-ci contrôle alors la validité de ce chiffre par rapport à sa table de *log-in*.

En plus de son authentification vis-à-vis du réseau S.W.I.F.T., la banque émettrice doit également s'authentifier vis-à-vis de la banque destinataire finale du message.

Cette authentification garantit que le message reçu n'a subi aucune altération accidentelle ou frauduleuse et qu'elle provient bien de l'émetteur autorisé. Une telle garantie est assurée par le procédé suivant : le calcul de l'authentificateur par la banque émettrice et son contrôle par la banque destinataire sont effectués par combinaison d'un nombre fixe d'authentification et de la totalité des caractères composant le texte du message (26).

Bien qu'ils offrent une grande sécurité, les systèmes cryptographiques à clés publiques présentent aussi d'importants inconvénients : leur installation est coûteuse et la procédure d'authentification est relativement lente.

(25) Voir notamment D. Syx, op. cit., Kredietbank, p. 246 sur la « Security-Key », du système Tele-Link.

(26) Un autre exemple original d'authentification est celui qui vient d'être mis au point par les banques belges (« TRASEC ») dont on trouvera une description dans le texte cité supra de Ph. Van Heurck.

C. — *L'AUTHENTIFICATION PAR RECONNAISSANCE DE CARACTERISTIQUES PHYSIQUES.*

Parmi les nombreuses méthodes de reconnaissance à distance de caractéristiques physiques, la plupart sont encore expérimentales. Il s'agit notamment, de la reconnaissance de l'iris, de la sueur, de la démarche, de la morphologie du visage, du sang, des cheveux, etc... Mises à part les difficultés techniques qui restent à résoudre pour les rendre opérationnelles, on remarquera que, sur le plan juridique, ces techniques sont comme telles incapables d'assurer les deux fonctions de l'authentification : identification et indication de la volonté d'appropriation. Elles ne permettent que la reconnaissance, c'est-à-dire l'identification. Pour remplir la deuxième fonction, elles devraient être combinées à un acte délibéré de la personne identifiée par laquelle elle marquerait sa volonté de faire le message sien (par exemple pour la reconnaissance par l'iris, l'obligation de poser l'œil à un endroit déterminé). Une technique, déjà opérationnelle qui remplit les deux fonctions est la reconnaissance dynamique de la signature, c'est-à-dire « l'authentification de la personne par le mouvement de son crayou lorsqu'elle signe » (27). Ce système est basé sur la comparaison, à partir de différents critères (vitesse pression, accélération...) par l'ordinateur d'une signature de référence stockée dans celui-ci et la signature apposée par la personne qui veut s'authentifier. Bien que ces systèmes offrent un haut degré de fiabilité (28), ils sont encore très peu répandus dans la pratique des affaires.

Par rapport aux autres techniques modernes d'authentification, les méthodes basées sur la reconnaissance de caractéristiques physiques offrent un grand avantage : elles permettent d'identifier et d'attribuer un message à une personne physique déterminée, et non pas seulement à un détenteur des moyens d'accès (par exemple un code secret).

III.— RECEVABILITE ET FORCE PROBANTE DES TECHNIQUES MODERNES D'AUTHENTIFICATION.

Nous avons déjà souligné que l'authentification revêt une fonction probatoire (29). Pour être susceptible de constituer la preuve d'une transaction en cas de différend quand à l'existence ou au contenu de celle-ci, l'authentification doit répondre à certaines exigences.

(27) Thierry Schwab et M. d'Alençon, op. cit., p. 61.

(28) Les tests effectués sur le nouveau système de reconnaissance dynamique de la signature I.B.M. (I.B.M. Dynamic Signature Verification) ont donné les résultats suivants : taux de vrais refusés 0,19 % taux de faux acceptés 0,56 %. (Informatique et systèmes, Janvier 1986 n° 1, p. 4.)

(29) Voir supra.

Il s'agit en premier lieu, d'exigences légales (A). Nous verrons qu'en droit privé français et belge celles-ci sont extrêmement limitées en matière de transactions commerciales.

Néanmoins, pour « emporter l'intime conviction du juge » saisi du litige, la partie qui se prévaut d'une transaction devra en rapporter une preuve convaincante. L'authentification devra donc, en second lieu, répondre à certaines exigenees pratiques de fiabilité. Nous examinerons au travers de quelques décisions de jurisprudence déjà rendues sur la question la réception par les juges des techniques modernes d'authentification (B).

Enfin, nous étudierons la possibilité pour des parties en relation d'affaires régulière par télématique de convenir entre elles des techniques d'authentification auxquelles elles entendent reconnaître une force probante privilégiée (C).

A. — *LES EXIGENCES LEGALES EN MATIERE DE PREUVE.*

Du point de vue des exigences légales relatives à la preuve, il y a lieu de faire une distinction fondamentale selon que l'on se trouve en présence d'un «fait juridique» ou d'un «acte juridique». En effet alors que le premier peut être prouvé par toute voie de droit (présomption, témoignage etc.) le second ne peut, en principe, être prouvé que par un écrit signé par application de l'article 1341, alinéa 1 du Code Civil (30). Ce qui distingue l'acte juridique du fait juridique, c'est que les conséquences de droit du premier sont indépendantes de la volonté de celui qui en fait l'objet (31). L'exécution d'un acte juridique est, selon certains auteurs, considérée comme un fait juridique (32) mais cela est controversé.

Les transactions télématiques appartiennent tantôt à la catégorie des actes juridiques et tantôt à celle des faits juridiques. Ainsi, la conclusion d'un contrat d'achat-vente par échange télématique de messages entre les parties constitue un acte juridique. Par contre, le paiement du bien acheté, via un transfert électronique de fonds devrait être rangé dans la

(30) L'article 1341 alinéa 1 du Code Civil belge dispose que : « Il doit être passé acte devant notaire ou sous signature privée de toutes choses excédant la somme ou la valeur de trois mille francs, même pour dépôts volontaires ; et il n'est reçu aucune preuve contre et outre le contenu aux actes ».

(31) Pour une discussion intéressante des notions complexes d'acte et de fait juridique, on se référera à Yves Poullet et Xavier Thunis, Introduction aux aspects juridiques de la télématique, in La Télématique, Aspects techniques, juridiques et socio-politiques, Actes du colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur, Story Scientia, Gent, 1984, tome I, p. 159.

(32) Voir à ce sujet N. Catala, La nature juridique du paiement, Paris, L.G.D.J., 1961.

catégorie des faits juridiques dans la mesure où il constitue l'exécution du contrat d'achat-vente par l'acheteur.

Lorsqu'elles appartiennent à la catégorie des actes juridiques, les transactions télématiques sont, en principe, soumises à l'exigence de l'écrit signé contenue dans l'article 1341 alinéa 1 du Code Civil. L'interprétation restrictive (33) donnée à cette disposition, en vertu de laquelle la signature doit être manuscrite pour assurer la présence physique à l'acte du prétendu signateur, l'élève en obstacle à l'utilisation de la télématique pour conclure des actes juridiques. L'avantage de la télématique est en effet de permettre la conclusion instantanée d'actes juridiques à distance, sans nécessiter la présence physique des personnes qui y sont parties. Certains pays envisagent une modification du Code Civil afin de supprimer cette difficulté. Tel est le cas du Grand-Duché de Luxembourg qui propose de définir la notion de signature dans le Code Civil de la façon suivante :

> « La signature consiste dans l'apposition par une personne de son nom ou de toute autre marque l'individualisant par laquelle elle manifeste son consentement ».

L'obstacle de l'exigence d'un écrit signé pouvant résulter de l'article 1341 alinéa 1 du Code Civil est considérablement limité dans ses effets par l'alinéa 2 de cette même disposition. Celui-ci restreint le champ d'application de l'alinéa 1er en énonçant que « (l)e tout (est) sans préjudice de ce qui est prescrit dans les lois relatives au commerce ». En vertu de ces lois (respectivement les articles 25 et 109 des codes de Commerce belge et français) les actes et engagements qui revêtent un caractère commercial (34) bénéficient du régime de la preuve libre.

En matière commerciale, tous les modes de preuve sont donc admissibles sous le contrôle du juge.

Le présent exposé étant consacré à l'étude des transactions *commerciales* assistées par ordinateur, il ne nous appartient pas d'étudier les difficultés éventuelles soulevées par la dématérialisation au regard des articles 1341 et suivants du Code Civil.

En vertu du principe de la preuve libre d'application en matière commerciale, toutes les techniques modernes d'authentification sont en principe recevables pour établir le contenu et l'existence de transactions commerciales.

(33) Voir à ce sujet : Cass. comm. fr., 19 novembre 1973, Bull. civ. 1973, n° 33 et M. Van Quickenborne, op. cit., p. 84 et les arrêts cités de la Cour de cassation - Contra, la position de D. Syx en faveur d'une interprétation fonctionnelle de la signature qui permettrait d'inclure dans cette notion certaines techniques modernes d'authentification (D. Syx, op. cit.).

(34) En vertu des articles 2 et 3 du Code de commerce.

Ce principe connaît certaines exceptions. Citons à titre d'exemples en droit belge : l'article 25 de la loi du 11 juin 1874 sur les assurances terrestres qui prévoit que le contrat d'assurance doit être prouvé par écrit ; un usage consacré comme source de droit par la Cour de cassation prévoit que les réclamations contre des factures importantes doivent être exprimées par écrit (35) ; l'article 3 de la loi du 25 octobre 1919 sur la mise en gage du fonds de commerce dispose que la validité de celui-ci est subordonnée à l'existence d'un écrit.

Si le principe permet la libre admissibilité des moyens de preuve, il réserve au juge le pouvoir d'en apprécier la force probante. Il convient donc d'examiner maintenant dans la jurisprudence la force probante qui peut être accordée aux techniques modernes d'authentification.

B. — *LES NOUVELLES TECHNIQUES D'AUTHENTIFICATION DANS LA JURISPRUDENCE*

Les propos d'un juge américain illustrent bien la problématique examinée dans la présente partie. Dans l'affaire *Perma Research and Development v. Singer Co.* (36) un document informatique avait été admis devant le tribunal. Cependant, un juge déclara au sujet de la fiabilité de ce document : « Ayant comme beaucoup d'autres citoyens reçu des factures informatisées pour des montants payés depuis longtemps, je ne suis pas prêt à accepter le produit d'un ordinateur comme la sainte écriture » (37).

La difficulté d'emporter l'intime conviction du juge sur base de la fiabilité d'une technique moderne d'authentification existe tant en droit anglo-saxon qu'en droit continental (38). Nous nous limiterons cependant dans le présent exposé à des exemples tirés de la jurisprudence en droit continental.

Il existe évidemment très peu de jurisprudence relative aux techniques les plus modernes d'authentification décrites ci-dessus (cryptographie codes secrets, reconnaissance de caractères physiques) (39). Notre analyse se référera donc à la jurisprudence qui a été rendue à

(35) Voir Cass., 29 mars 1976, Pas., 1976, II, 833.
Pour plus de détails, voir X. Dieux, La preuve en droit commercial exposé au congrès de l'I.D.E.F., Bruxelles, 1984.

(36) 452 F II 2d Cir. 1976.

(37) Ibidem, Dissenting Opinion du Juge Van Graafeiland.

(38) Voir à ce sujet Bernard Amory et Yves Poullet, Le droit et la preuve face à l'informatique et à la télématique, Revue internationale de Droit comparé, 2, 1985, p. 331 à 352.

(39) Voir supra.

propos d'autres techniques d'authentification un peu moins récentes. Il s'agit principalement de celles utilisées pour les transactions effectuées par télex ou par téléphone.

La jurisprudence française tient compte de la pratique devenue courante dans le monde des affaires de conclure des contrats par télex en leur accordant un haut degré de fiabilité (40). En Belgique, il n'existe, à notre connaissance, aucune jurisprudence concernant la fiabilité du télex en matière commerciale. Cette absence de contestation est peut-être une preuve de la confiance accordée par le monde des affaires à l'authentification par télex. L'exemple de l'Italie est intéressant. En vertu du décret présidentiel n° 735 du 7 février 1963, un contrat conclu par télex est assimilé à un contrat par écrit à condition, d'une part, que l'utilisateur du télex s'identifie correctement en donnant à la fin de chaque communication son numéro de télex et le code correspondant et, d'autre part, qu'il conserve la copie de tous les télex envoyés et interdise l'utilisation de son installation par des tiers. Un jugement du Tribunal d'Ascoli-Piceno (41) a appliqué et précisé ces dispositions législatives en considérant que puisque le message télex identifie le télescripteur qui a produit le texte et que cet appareil est à la disposition exclusive de l'expéditeur, celui-ci est présumé être le titulaire de l'installation. Selon le tribunal cette présomption est réfragable par exemple au moyen de la facture des P.T.T. En effet étant donné que celle-ci reprend le détail du jour, de l'heure et de la durée des communications par télex, elle pourrait établir, dans certains cas, que ce n'est pas le titulaire de l'installation qui a envoyé le message.

A propos des transactions conclues par téléphone, un arrêt de la Cour de cassation française (42) va à l'encontre de la jurisprudence évoquée ci-dessus à propos du télex.

Dans cette affaire, un journal prétendait avoir reçu commande par téléphone pour diverses annonces publicitaires. La société titulaire et utilisatrice des installations téléphoniques correspondantes prétendait n'avoir jamais commandé ces annonces publicitaires et refusait de les payer. Le Tribunal saisi de l'affaire condamna la société utilisatrice à payer ces commandes d'annonces publicitaires au motif que cette société avait la garde de son installation téléphonique et devait donc en contrôler l'utilisation.

(40) Voir Annayme, Telex contracts - a comparative study, International Financial Law Review, May 1982, p. 22 à 29 et la jurisprudence citée.

(41) Bouhassira/S.A.R.L. Régie Print, Cour de cassation, Ch. comm. 11 juin 1981, Bull. Civ. Com. N° 265 p. 211. Cet arrêt est rapporté et commenté dans un très intéressant article de A. Bensoussan dans 01 Informatique, mars 1984, n° 178, p. 75.

(42) Soc. Socona v. Soc. Sider-Tronto, Tribunale Ascoli Piceno 7 septembre 1980, European Commercial Cases, Vol. V, July 1982, p. 317.

La Cour de cassation refusa d'entériner ce raisonnement et cassa le jugement.

On constate donc que la jurisprudence accorde un haut degré de force probante au télex, technique actuellement largement utilisée pour effectuer des transactions commerciales. Par contre, le téléphone qui offre moins de garanties de fiabilité (pas de possibilité d'identification automatique et certaine de l'expéditeur du message) n'obtient pas le même degré de force probante.

C. — *CONVENTIONS RELATIVES A L'AUTHENTIFICATION.*

Nous avons vu que la jurisprudence accorde un haut degré de force probante à des techniques d'authentification modernes mais déjà très largement utilisées dans la pratique.

Le degré de force probante qu'accorderait un tribunal à une technique d'authentification encore plus moderne mais moins répandue (comme la cryptographie ou la reconnaissance de caractères physiques) est incertain. Pour éliminer cette incertitude, les parties peuvent, en vertu de l'article 1134 du Code Civil, convenir entre elles par écrit et sous forme traditionnelle de donner une force probante privilégiée à la technique particulière qu'elles utilisent pour les transactions télématiques. Il est, en effet, généralement admis que l'article 1341 du Code Civil n'est ni d'ordre public ni impératif (43).

Une telle convention n'est évidemment concevable qu'entre parties en relation d'affaires régulière. Par analogie avec la jurisprudence sur les ordres de virement donnés par télex (44) une convention relative à l'authentification ne libérerait pas le destinataire d'un message, reçu conformément à la procédure d'authentification convenue, de ne pas lui donner une suite favorable s'il apparaît au vu de son contenu et des circonstances que le message ne peut avoir été envoyé par l'expéditeur autorisé.

La convention relative à l'authentification pourra, par exemple, faire l'objet d'une clause dans la convention de base entre une banque et une entreprise relative à un service de gestion des comptes par télématique. Une telle clause peut également figurer dans un règlement

(43) Voir X. Malengreaux, Le droit de la preuve et la modernisation les techniques de rédaction de reproduction et de conservation des documents, Annales de Droit de Louvain, 1982, p. 117 et les références citées sous (28). Voir aussi Cass. Franc., 7 janvier 1982, Bull. Cass., 1982, III, 4.

(44) Voir D. Carton, Aspects juridiques des ordres de virement transmis par télex, D.I.S.E.P., vol. I, n° 2 octobre 1985, p. 3.

anquel adhèrent les banques participuntes à un réseau de transferts électroniques de fonds ou de transfert d'informations financières. On notera qu'il est utile que les parties conviennent également de la durée peudant laquelle elles conserveront les documents laissant une trace des techniques d'authentification utilisées.

On constate donc que les arrangements contractuels permis par le Code Civil donnent aux entreprises désireuses de s'eugager dans des transactions télématiques d'une part une grande liberté quant aux moyens d'authentification et d'autre part suffisamment de sécurité juridique. Bien enteudu, de tels aménagements conventionnels ne sont valables qu'entre parties. Toutefois, si une technique d'authentification est adoptée par un ensemble d'entreprises, par exemple la communauté bancaire, il est fort probnble qu'elle soit objectivement fiable et qu'un tribunal y accorderait en l'absence de conventiou à cet effet, une force probante privilégiée.

SECTION 2

QUESTIONS DE RESPONSABILITE SOULEVEES PAR LES TRANSACTIONS COMMERCIALES ASSISTEES PAR ORDINATEUR

Le schéma complexe présenté pour illustrer les problèmes d'authentification posés par les transferts électrouiques de fouds a fait ressortir la multiplicité des parties à l'opération, multiplicité qui complique singulièrement le règlement des questions de responsabilité.

I. — LA TRANSACTION A DISTANCE : LES ACTEURS.

Nous proposons d'nbord un schéma simplifié qui a l'avantage de faire ressortir les rapports fondamentaux caractérisant toute opération à distance, qu'elle utilise le télex, le téléphone ou la voie télématique (télécommunications plus informatique).

L'opération à distance, télématique en particulier, met en présence au moins trois acteurs selod le schéma suivant :

Transporteur du message

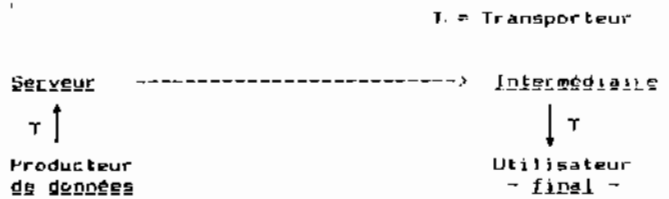
Emetteur du message ——————→ Destinataire du message

A. — *L'EMETTEUR ET LE DESTINATAIRE DU MESSAGE*

a) L'émetteur peut être une *entreprise* (45) qui utilise le réseau de télécommunications pour passer une commande de biens ou de services dont les caractéristiques sont transmises à distance. Ce peut être aussi inversement une entreprise qui a fait offre pour les biens qu'elle produit ou les services qu'elle fournit. Le destinataire sera bien évidemment l'entreprise fournisseur ou, inversement, l'entreprise qui accepte l'offre.

b) L'émetteur du message n'est pas nécessairement unique et il est fréquent que plusieurs personnes physiques et/ou morales contribuent à la production de l'information qui circulera dans le réseau.

b1) Il en est ainsi dans le domaine des banques de données où l'émetteur d'informations est souvent constitué par le producteur de données et le serveur (46) qui en assure la distribution (47). Si les producteurs de données travaillent en amont des serveurs, des intermédiaires interviennent parfois entre le serveur et le destinataire final de l'information pour sélectionner le type d'informations utiles (48).



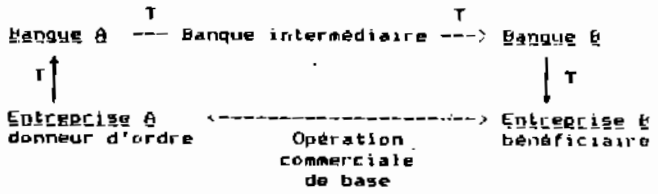
b2) Il en est également ainsi dans un transfert électronique de fonds du client donneur d'ordre et de la banque émettrice ou transférante, le destinataire étant constitué dans ce cas de la banque réceptrice et de sa cliente bénéficiaire du transfert.

---

(45) Rappelons que nous ne traitons pas des problèmes juridiques posés par la télématique grand public.

(46) Le producteur peut aussi être son propre serveur : il est alors appelé serveur intégré.

(47) (48) Pour une définition plus précise des concepts de producteur et de serveur, voir Y. Poullet et X. Thunis, Introduction aux aspects juridiques de la télématique in La Télématique, aspects techniques, juridiques et socio-politiques, Story Scientia, 1984, p. 129 et s.



B. — *LE TRANSPORTEUR D'INFORMATIONS*

Le transporteur gère la liaison et assure la transmission entre l'émetteur et l'utilisateur d'informations. Une liaison entre utilisateur et émetteur peut nécessiter l'intervention de différents transporteurs, par exemple en matière de flux transfrontières.

On peut distinguer plusieurs types de transporteurs : les transporteurs privés, les transporteurs publics et les transporteurs « mixtes » constitués sous la forme de société d'économie mixte où se retrouvent à la fois le privé et le public.

Il semble que la responsabilité du transporteur dépende moins de sa forme juridique, publique, privée ou mixte que du type de service qu'il assure. Si l'on admet que la responsabilité du transporteur soit minimale pour des services de télécommunication *de base*, on peut soutenir que celle-ci doit être plus étendue pour des services de télécommunication à *valeur ajoutée* c'est-à-dire des services impliquant la modification (exemple le codage) de l'information transmise (49).

Par ailleurs il arrive que les lignes permettant le transport d'informations soient données en location par les P.T.T. à une entreprise privée (50). C'est souvent le cas dans les systèmes de transmission de données financières qui fournissent à l'heure actuelle l'exemple le plus significatif de transactions dématérialisées. Nous y limitons notre analyse.

(49) Sur la distinction entre services de télécommunications de base et services de télécommunication à valeur ajoutée, voir Y. Poullet et B. de Crombrugghe, La réglementation des télécommunications en Belgique, colloque de l'A.B.U.T. octobre 1985, p. 62 et s.

(50) Pour plus de détails, voir Y. Poullet, op. cit. p. 17 et s.

II. — LA TRANSACTION FINANCIERE (51) A DISTANCE : LES DOMMAGES.

A. — *RISQUES POSSIBLES. DOMMAGES REPARABLES.*

On sait qu'en droit, pour que la responsabilité d'une personne puisse être mise en cause, il est nécessaire que son acte *fautif cause* à autrui un *dommage* qui est la condition première de l'obligation de réparer.

Quels sont les risques inhérents aux systèmes de communication de données à distance et leurs conséquences dommageables dans le cas plus particulier d'un réseau de communication de données financières.

1° L'altération du message transmis qui arrive incomplet ou falsifié à son destinataire.
2° La transmission d'un message à un destinataire erroné.
3° L'expédition du message par un expéditeur non autorisé.
4° Le retard dans la transmission du message.

La réalisation d'un ou plusieurs de ces risques qui peuvent résulter d'une fraude, d'une négligence ou d'une erreur, donnera lieu en principe à un dommage qu'il faudra faire supporter, autrement dit imputer à une des parties de l'opération (voir *infra* III).

Le participant à un réseau de télématique financière (tel que S.W.I.F.T. par exemple) peut subir quatre types de dommages.

1) *La perte du montant principal* (en tout ou partie)

Celle-ci peut se produire lorsqu'un transfert électronique est crédité à un compte qui n'est pas le bon, crédité au bon compte pour un montant excessif ou effectué deux fois, et que le bénéficiaire retire les fonds qu'il ne peut plus restituer (52).

2) La *perte d'intérêts.*

Celle-ci résulte de retards apportés au transfert, soit du fait des banques, soit encore du fait de leurs clients qui ont tendance, pour des raisons de trésorerie, à retenir l'ordre de transfert jusqu'au dernier moment.

(51) Pour une présentation générale des problèmes évoqués au texte, voir N.U. Projet de guide juridique sur les transferts électroniques de fonds A/CNo/250/Add. 1 et s.

(52) Sur ce problème et pour des exemples, voir H. Lingl, Risk allocation in International Interbank Electronic Fund Transfers Chips & S.W.I.F.T., I.I.R. 1981, n° 3 p. 630 et s. plus particulièrement la note 124.

3) *Pertes dues aux taux de change.*

Celles-ci se produisent quand un retard dans le transfert est couplé à une fluctuation dans le taux de change.

4) *Dommages indirects (consequential damages).*

Le projet de guide juridique sur les transferts électroniques de fonds cite, à titre d'exemple de dommages indirects, la perte d'un contrat ou l'imposition d'une pénalité à charge du transférant parce que l'ordre de paiement n'a pas été traité correctement.

Toujours selon le projet de guide juridique, la banque du transférant ne serait pas tenue pour responsable des dommages indirects imprévisibles lorsqu'elle a reçu l'ordre de transfert de fonds du transférant, à moins qu'elle n'ait fait preuve de dol dans l'exécution de l'ordre. Cette assertion doit, en droit français et belge tout au moins, être nuancée car elle confond à notre avis plusieurs ordres d'idées.

B. — *LE DOMMAGE REPARABLE, RAPPEL DES PRINCIPES.*

1° En matière contractuelle, les articles 1150 et 1151 du Code Civil établissent deux principes importants :

a) sont seuls dus les dommages-intérêts qui ont été prévus ou que le débiteur a pu prévoir lors du contrat, à moins qu'il ne s'agisse d'une inexécution intentionnelle (art. 1150),

b) le débiteur, même en cas de faute intentionnelle n'est jamais tenu du dommage indirect (art. 1151).

Comme le fait remarquer De Page (53), prévisibilité du dommage et dommage indirect sont deux ordres d'idées différents.

Il est normal que les parties qui ont adhéré librement à un engagement limitent leurs calculs à ce qu'elles peuvent normalement prévoir, le tout étant de déterminer, *en fait*, ce qui est prévisible (54).

Par contre en matière extra contractuelle, toutes les répercussions dommageables d'un acte prévisibles et imprévisibles, doivent être réparées. Cette remarque peut avoir son importance en cas de recours d'un donneur d'ordre contre une banque avec laquelle il n'a pas de lien contractuel direct.

(53) H. de Page, Traité élémentaire de droit civil belge t. IV Bruylant 1940 n° 1023 et s.

(54) Ainsi, dans le domaine des banques de données juridiques, l'utilisateur qui, par suite d'une information déficiente, perd « le procès du siècle », subit un dommage qui est une suite immédiate et directe de l'inexécution de la convention. Mais ce dommage est-il prévisible à la conclusion du contrat ?

En tout cas, si par dommage indirect on vise un dommage qui n'est pas une suite nécessaire de la faute, la relation causale avec celle-ci fait défaut. Le dommage qualifié indirect, n'est donc pas indemnisable (55).

Il n'est pas certain, à la lumière des principes rappelés ci-dessus, que les exemples cités par le Projet de Guide Juridique constituent des dommages indirects, ni même des dommages imprévisibles quant à leur principe.

2° Puisque le dommage imprévisible (56) n'est en principe pas couvert, le transférant (57) pourrait notifier à la banque transférante les conséquences d'une inexécution ou d'une exécution tardive à l'ordre de transfert. La banque ainsi informée ne pourrait se prévaloir de l'imprévisibilité du dommage, ce qui présente l'avantage pour le transférant de diminuer les risques de non indemnisation.

On signale, à juste titre, que ces informations ne sont généralement pas communiquées, ni à la banque intermédiaire, ni à la banque bénéficiaire. Rien n'empêche cependant, malgré certaines difficultés techniques relevant notamment de la normalisation des messages qu'elles soient ajoutées aux instructions envoyées par la banque expéditrice (58). Si la banque intermédiaire ou la banque bénéficiaire n'en tiennent pas compte, erreur ou négligence, le recours du transférant contre sa banque risque de s'avérer improductif, car cette dernière va invoquer la faute d'un tiers sauf, conformément à la suggestion formulée par certains auteurs (59) à propos du transporteur, à rendre la banque transférante responsable de la totalité du réseau (pour plus de détails voir *infra).*

3° Enfin, il ne faut pas perdre de vue l'article 1153 du Code Civil qui, pour les obligations portant sur le paiement de sommes d'argent, établit que les dommages et intérêts résultant du retard dans l'exécution ne consistent jamais que dans les intérêts légaux. Les parties peuvent cependant par convention stipuler que les dommages intérêts moratoires excèderont le taux légal (60).

(55) Sur le rapprochement entre responsabilité contractuelle et délictuelle pour l'appréciation du lien de causalité et l'adoption du critère de nécessité, P. Van Ommeslaghe, La responsabilité contractuelle in Les obligations contractuelles, Editions du Jeune Barreau 1984, p. 243 et s.

(56) M. Dalcq dans son Traité de la responsabilité civile, Larcier 1962 t. II, n° 2372, fait justement observer que la règle de l'article 1150 du Code Civil, ne concerne que l'étendue de la réparation et non l'existence même du dommage.

(57) Pour une suggestion semblable dans le domaine des banques de données, Y. Poullet et X. Thunis, op. cit., p. 172.

(58) A ce sujet, Projet de guide juridique déjà cité, p. 27 spécialement n° 99 et s.

(59) M. Vasseur, Aspects juridiques des nouveaux moyens de paiement, revue de la banque 1982, 592.

(60) H. De Page, Traité élémentaire de droit civil belge, Bruxelles, Bruylant 1940, t. IV, n° 142 et s.

III. — LA TRANSACTION FINANCIERE A DISTANCE : IMPUTATION DES RESPONSABILTES.

Après le dommage, nous examinons sous une même rubrique les deux autres éléments constitutifs de la responsabilité, la faute et le lien de causalité, éléments difficilement séparables, l'appréciation de la faute influant sur l'établissement du lien causal.

Nous exposerons successivement les problèmes de responsabilité dans la relation entre le créancier et son débiteur qui est aussi le donneur d'ordre (A). Les rapports de ce dernier avec sa banque (B) seront également examinés et une attention particulière sera consacrée à la responsabilité de la banque transférante pour tout le réseau (C). Les relations interbancaires, qui ne constituent pas l'objet central de cette étude, seront brièvement mentionnées (D).

A. *LA RELATION DONNEUR D'ORDRE-CREANCIER.*

En vertu de l'opération commerciale de base le créancier (l'entreprise B dans notre schéma *supra*), a droit à un paiement en espèces qui est la contre-partie de la prestation, fourniture de biens ou de services, qu'il a lui-même effectuée sur base du contrat qui le lie à son débiteur (l'entreprise A dans notre schéma).

1° *Les dommages du créancier : roppel.*

Plusieurs situations dommageables pour le créancier peuvent se présenter :

1) Il ne reçoit pas le principal de la créance pour des causes qui peuvent être en fait très diverses : le débiteur est insolvable ou déclaré en faillite ; de mauvaise foi ou négligent, il omet de donner l'ordre de transfert ou, encore, l'ordre de tranfert aboutit à créditer un compte qui n'est pas le bon.

2) Il reçoit le principal, mais avec retard. La notion même de retard suppose que l'on puisse déterminer avec précision le délai dans lequel doit s'effectuer le paiement, soit dans les rapports entre le créancier et le débiteur le délai fixé contractuellement, soit dans les rapports entre le débiteur et sa banque (banque transférante), le délai « normal » dans lequel celle-ci doit exécuter l'ordre de paiement.

Le dommage consistera dans la perte d'intérêts si l'opération est internationale dans la perte due aux fluctuations dans le taux de change entre le moment où le paiement aurait dû être effectué et le moment où il a réellement été effectué.

Par application de l'article 1153 du Code Civil, le créancier ne peut réclamer que des intérêts moratoires calculés au taux légal. Il s'agit là d'un principe et la pratique contractuelle montre que les parties prévoient souvent un régime plus sévère pour le débiteur défaillant, l'article 1153 n'étant qu'une disposition supplétive de volonté.

On n'oubliera pas par ailleurs que le transfert électronique de fonds revêt le plus souvent un caractère international et que le droit applicable à cette opération ne sera pas nécessairement le droit civil tel que l'exprime le Code Napoléon soit qu'un système juridique différent ait été expressément désigné par les parties, soit que les éléments de l'opération tels que le lieu de son exécution... conduisent à régler les difficultés éventuelles en dehors du système prévu à l'article 1153.

2° *Imputation de la responsabilité.*

En droit, du point de vue du créancier ou ayant droit au paiement, les causes du non paiement ou d'un paiement tardif peuvent être de deux types.

1) Causes imputables au débiteur.

Le donneur d'ordre qui émet un transfert par télétransmission parce qu'il a une obligation envers le bénéficiaire est responsable envers celui-ci de la bonne exécution de l'ordre et ne peut se prévaloir d'une défaillance de sa banque ou d'un établissement transmetteur situé en aval. Ceci signifie concrètement que le donneur d'ordre vis-à-vis du bénéficiaire supporte les conséquences d'une exécution tardive de l'ordre ou d'une inexécution provenant d'une faute de sa banque (exemple : exécution tardive ou incorrecte d'un ordre correct ou donné dans les délais par le débiteur).

2) Causes non imputables au débiteur.

L'obligation de paiement (compris au sens commun comme l'obligation d'apurer une dette d'argent) pesant sur le débiteur est une obligation de résultat. Le prescrit de l'article 1147 du Code Civil s'applique donc suivant lequel « le débiteur est condamné s'il y a lieu au paiement de dommages et intérêts... toutes les fois qu'il ne justifie pas que l'inexécution provient d'une cause étrangère qui ne peut lui être imputée... ». Rentrent sous le concept de cause étrangère exonératoire, la force majeure (a), le fait d'un tiers (b) et le fait du créancier lui-même (c).

a) Selon la Cour de cassation belge, « *la force majeure* » qui libère le débiteur de l'obligation de payer des dommages et intérêts suppose un événement créant un obstacle insurmontable à l'exécution par

celui-ci de ses obligations, et non imputable quant à sa cause à une faute quelconque du débiteur » (61). L'impossibilité d'exécution doit être appréciée raisonnablement (62).

A notre avis, la force majeure n'aura qu'un rôle secondaire dans la matière des transferts électroniques de fonds. Supposons, en effet, la faillite d'une banque intermédiaire ou, cas plus net encore, une défaillance du réseau de télécommunication. Cette défaillance imprévisible, indépendante du fait du débiteur, ne rend pas l'exécution de son obligation de paiement impossible puisque d'autres formes alternatives de règlement, tel l'envoi d'un chèque, demeurent possibles. Au mieux le débiteur pourra-t-il se prévaloir de la cause étrangère pour justifier un certain retard dans le paiement.

b) *Le fait d'un tiers* est en principe une cause étrangère exonératoire à la condition que le débiteur ne soit pas responsable de ce tiers. La jurisprudence belge considère que le débiteur (l'entreprise A dans notre schéma) est tenu de l'exécution de ses obligations envers son contractant, même s'il a recours à un agent d'exécution à cet effet. Ainsi la banque du débiteur, ou une banque intermédiaire choisie par la banque du débiteur, sont des tiers que directement ou indirectement celui-ci a engagé pour rendre possible l'exécution de son obligation de payer. Il est donc responsable vis-à-vis de son créancier (l'entreprise B dans notre schéma) (63). Nous verrons que cette « responsabilité contractuelle pour autrui » trouve aussi à s'appliquer dans les rapports entre le donneur d'ordre et sa banque (la banque A dans notre schéma).

c) *Le fait du créancier*. Il est compréhensible que le fait fautif du créancier exonère le débiteur de sa responsabilité, partiellement ou totalement. Par application de ce principe, à notre avis, le donneur d'ordre ne doit pas supporter le risque d'une défaillance de la banque de son créancier (la banque B dans notre schéma). Que l'on considère ou non celle-ci comme mandataire du créancier pour la réception des paiements (64), il n'en reste pas moins qu'elle a été choisie et désignée au donneur d'ordre par le créancier qui est tenu d'assumer les conséquences de son choix.

(61) Cass. 9 déc. 1976, Pas. 1977, I, 408.

(62) Pour plus de détails, M. Fontaine in «Les obligations contractuelles», Ed. du Jeune Barreau, 1984, p. 188.

(63) Pour plus de détails, P. Van Ommeslaghe, examen de jurisprudence, Les obligations (1974 à 1982) R.C.J.B. 1986 p. 212. Voir aussi J.L. Fagnart et M. Deneve, chr. de jurisprudence «La responsabilité civile» (1976-1984) J.T. 1985 p. 453 et s.

(64) Pour une discussion de la qualité du banquier du bénéficiaire, d'une part mandataire substitué du premier banquier, d'autre part mandataire à l'encaissement, voir A. Bruyneel, Le virement in La Banque dans la vie quotidienne. Ed. du Jeune Barreau 1986 p. 347 et s. spécialement notes (103) (111) et (118).

Comme le suggère l'exposé, le donneur d'ordre est le seul répondant vis-à-vis du créancier de la bonne exécution du transfert ; les banques intermédiaires sont ses auxiliaires, même s'il n'entretient de relations contractuelles qu'avec sa propre banque. La conséquence logique en est que le risque de non paiement ou de retard dans le paiement doit rester à charge du débiteur sous réserve d'une défaillance de la banque du bénéficiaire (65).

B. — *LA RELATION DU DONNEUR D'ORDRE AVEC SA BANQUE.*

Une fois posée, en principe, la responsabilité du donneur d'ordre vis-à-vis de son créancier il faut ensuite déterminer qui du donneur d'ordre ou de la banque va *in fine* supporter le dommage consistant dans la perte d'intérêts dont le bénéficiaire réclame le versement ou, plus grave, dans la perte de capital dont le donneur d'ordre est redevable vis-à-vis du bénéficiaire. Ou encore, hypothèse plus lourde de conséquences pécuniaires pour la banque, celle-ci va-t-elle devoir indemniser le donneur d'ordre parce que le transfert, erroné ou tardif, a provoqué la perte ou la rupture d'un contrat dont le donneur d'ordre attendait de substantiels profits.

La réponse à ces questions se trouve dans les principes généraux (qui a commis une faute et le dommage est-il une suite nécessaire de cette faute ?) dont les parties peuvent moduler l'application au cas d'espèce par des stipulations contractuelles particulières (clauses d'exonération notamment).

Les transferts électroniques de fonds ont souvent été rapprochés de la figure du virement bancaire et d'excellents auteurs (66) ont parlé de virement électronique.

L'exposé qui suit et les solutions proposées tirent largement parti de ce rapprochement qui paraît justifié puisque le virement de fonds est une opération par laquelle les banques permettent à leurs clients de mobiliser des fonds au départ d'un compte pour créditer un autre compte.

Seule change, en définitive, la façon dont les fonds sont mobilisés.

Si l'on reprend les quatre hypothèses de risques évoquées plus haut et qu'on les regroupe pour les besoins de l'analyse, on peut dis-

(65) En ce sens, voir le commentaire de la recommandation n° 4 du projet de résolution du comité de droit monétaire concernant le moment de l'exécution d'une dette d'argent.

(66) M. Vasseur, art. cité dans la Revue de la Banque.

tinguer (67) les transferts régulièrement ordonnés *(authorized transfers)* et les transferts irréguliers *unauthorized transfers)* (67 bis).

B1. — *LES TRANSFERTS REGULIEREMENT ORDONNES.*

Les transferts régulièrement ordonnés sont ceux qui portent sur des transactions non entachées de fraude ou d'erreur mais qui, soit ne sont pas exécutés par la banque du donneur d'ordre, soit sont exécutés tardivement.

1° *Les principes.*

1) Il n'y a pas beaucoup de problèmes quand il est établi qu'il y a violation fautive par la banque transférante elle-même de l'obligation d'exécuter un ordre de transfert née du contrat qui la lie à son donneur d'ordre, mais une hypothèse aussi nette est rare en pratique. La banque doit, comme pour les virements classiques, exécuter l'ordre de transfert avec « promptitude », ce qui pose la question du délai normal d'exécution et de la preuve de la date de réception de l'ordre.

2) L'inexécution de l'ordre, ou le retard dans son exécution, peuvent provenir du donneur d'ordre lui-même qui transmet son instruction « in extremis » ou dont le compte est insuffisamment provisionné, ce qui justifie un traitement différé de la banque. Il faudra examiner, dans le cas d'espèce, si la faute du donneur d'ordre est concurrente, voire même exclusive, de celle de la banque (69).

3) La force majeure est, selon le droit commun, une cause exonératoire de responsabilité. Les contrats passés entre les banques et les entreprises clientes en précisent l'étendue (ci-dessous).

2° *Les « contrats de transferts électroniques de fonds ». Examen de quelques clauses.*

Rien n'empêche les parties, par application du principe de la liberté des conventions (Code Civil article 1134) de restreindre ou d'élargir le concept de cause exonératoire :

1) Une première clause, classique, précise que la banque s'engage à apporter tout soin et diligence à l'exécution des prestations objets des présentes. Toutefois, la responsabilité de la banque ne saurait être engagée pour toutes erreurs ou anomalies dues aux défaillances et au *mauvais fonctionnement des réseaux publics de transmission.*

(67) Nous reprenons la distinction du Professeur Scott sur Les transferts interbancaires par télétransmission aux Etats-Unis Rev. int. de comp. 1985, n° 4.
(67 bis) Il est entendu qu'un transfert régulièrement ordonné peut ensuite faire l'objet d'une fraude et devenir un transfert irrégulier.
(68) Sur ces questions, voir A. Bruyneel, op. cit., p. 425 et s.
(69) Sur les virements exécutés sans provision, voir A. Bruyneel, op. cit. n° 49.

Il n'y a pas là d'extension significative par rapport au droit commun.

2) Un deuxième type de clauses élargit sensiblement la notion de force majeure en indiquant par exemple que « la banque ne peut en aucun cas être tenue pour responsable d'une interruption temporaire du service due à des événements indépendants de sa volonté comme par exemple une panne, une coupure des lignes téléphoniques des grèves ou des circonstances justifiant une telle interruption notamment des travaux visant à améliorer l'appareillage existant. La banque prendra toutefois toutes les mesures en son pouvoir pour limiter au maximum de telles interruptions ».

La grève ne constitue pas automatiquement un cas de force majeure (70), mais les parties peuvent prévoir que toutes les grèves seront considérées comme cause exonératoire.

Quant à la panne, de quel type de panne s'agit-il ? Panne d'électricité ? incendie ? panne d'ordinateur, erreurs dans un logiciel bloquant tout un système de traitement ?

Cette dernière hypothèse constitue incontestablement un élargissement de la force majeure auquel le donneur d'ordre sera attentif.

Le principe, à notre avis, devrait être que la banque doit disposer d'un équipement de remplacement suffisant *(« back up »)* pour permettre au système de continuer à fonctionner.

3) Un troisième type de clauses, beaucoup plus subtil, indique que le client et la banque conviennent expressément que tout préjudice financier ou commercial (par exemple, perte de bénéfice, trouble commercial quelconque) ou toute action contre le client par un tiers constitue un dommage indirect et par conséquent n'ouvre pas droit à réparation, même si la banque a été avisée de la possibilité de la survenance de tels dommages.

Le dernier membre de phrase vise expressément l'initiative qu'aurait prise le client de notifier à sa banque les conséquences dommageables d'une éventuelle inexécution de son ordre, conséquences devenant de ce fait prévisibles. (Sur cette question, voir nos considérations *supra).*

L'exonération stipulée au profit de la banque est ici très large, mais néanmoins valable puisqu'elle ne s'affranchit pas de son dol ou de sa faute lourde et qu'il n'est pas porté atteinte à l'objet même de l'obligation.

(70) A ce sujet P. Van Ommeslaghe, examen de jurisprudence cité, n° 106 p. 218.

B2. — *LES TRANSFERTS IRREGULIERS (71).*

Un transfert est irrégulier s'il a été ordonné par une personne non autorisée par le titulaire du compte ou si un des éléments du transfert tel que montant, destinataire, date de valeur... a été volontairement ou involontairement altéré. La fraude ou l'erreur peuvent donc être à l'origine d'un transfert irrégulier.

Plusieurs cas de figures peuvent être envisagés qui mettent en cause, soit la responsabilité du client, soit la responsabilité de sa banque.

1° Des employés malhonnêtes du client d'une banque, non habilités, émettent des ordres de transfert au nom de l'employeur en utilisant un terminal situé dans l'établissement du client. On encore, des employés habilités émettent un ordre de transfert électronique au bénéfice d'une personne qui n'y a pas droit (72).

La fraude n'est pas la seule origine de l'irrégularité d'un transfert. Il arrive que par l'entreprise donneur d'ordre, par l'entremise d'un de ses employés ou mandataires, commette une erreur ou ne soit pas suffisamment complète dans les instructions données à la banque.

2° Le transfert, bien que l'ordre soit régulier dans le chef du client, est exécuté erronément par la banque qui, par exemple, crédite un compte autre que celui du véritable ayant droit.

L'hypothèse d'une fraude dans le chef des employés de la banque ou même de tiers est également envisageable.

Sans prétendre être exhaustif dans l'analyse des problèmes de responsabilités (73), nous énonçons ci-après les principes qui doivent guider la recherche d'une solution (a). Référence sera faite à des conventions ou à des « règlements » existants (b).

a) *Les principes :* Bien que les « contrats de transferts électroniques de fonds » et les règlements généraux d'opérations comportent des dispositions réglant le partage des responsabilités entre la banque et son donneur d'ordre, il semble utile, ne fût-ce que pour prendre l'exacte mesure des dérogations contractuelles, de rappeler que, dans la matière des virements, le banquier qui reçoit un ordre de son client est tenu de le vérifier encore que l'étendue et l'objet de cette obligation soient peu précisés.

(71) Pour plus de détails sur les exemples cités au texte voir N.U. doc. cité n° 5 et s. n° 23 et s. Sur les virements effectués par erreur, Van Ryn et Heenen, Principes de droit commercial, t. III, Bruylant, Bruxelles 1960 n° 2063 et s.

(72) Ceci suppose évidemment que les procédures de contrôle et de sécurité (mots de passe, code secret...) aient été faussés ou se soient avérés inefficaces.

(73) Des enseignements intéressants peuvent être tirés de la matière des virements. Voir à ce sujet l'étude très détaillée déjà citée de A. Bruyneel p. 418 et s.

Les procédures de sécurité et de reconnaissance appliquées par les banques dans le domaine des transferts électroniques de fonds doivent concourir à la bonne exécution de cette obligation, un des problèmes rencontrés étant de déterminer qui, du client ou de sa banque, supporte les conséquences d'un niveau de sécurité insuffisant.

b) *La pratique contractuelle.*

1) La clause suivante illustre fidèlement la façon dont les contrats règlent l'hypothèse de la fraude :

> « Les conséquences directes ou indirectes pouvant éventuellement découler de l'emploi abusif du service, soit par des utilisateurs désignés, soit par des tiers, ne peuvent être mises à charge de la banque. Par la présente, l'abonné reconnaît assumer l'entière responsabilité d'une telle utilisation abusive. »

Le client est responsable du comportement frauduleux de ses employés, habilités ou non, et même des tiers. Son compte pourra être débité du montant des transferts effectués sur la base d'ordres même falsifiés. Le fondement de la responsabilité mise à charge du client pourrait être recherché dans le concept classique de faute (74), bien qu'une approche en terme de risque semble plus adéquate.

Ce type de solution « compréhensible » puisque le client a ou devrait avoir la maîtrise des lieux d'où émane l'ordre de transfert, devrait cependant être nuancé.

a) La transaction ne doit pas revêtir un caractère manifestement inhabituel auquel cas elle devrait attirer l'attention de la banque. Le caractère manifestement inhabituel d'une transaction peut s'induire de montants plus élevés que ceux généralement ordonnés ou encore de destinataires totalement inconnus jusque là...

b) La fraude peut avoir été rendue possible par une insuffisance du système de sécurité mis en place par la banque aux instructions de laquelle le client s'est conformé. Dans ce cas, la responsabilité de la banque nous semble engagée, car s'il est vrai que le client (une entreprise et donc un « professionnel ») a le choix d'un mode de paiement, il est tout aussi vrai que le banquier, en tant qu'organisme de crédit professionnel, est, en première ligne, responsable du système informatique qu'il propose pour l'organisation et la rationalisation des services bancaires.

(74) Pour les banques de données, Y. Poullet et X. Thunis, op. cit., p. 156 : « Le risque... pourrait être mis à la charge du titulaire des moyens d'accès, soit à titre de sanction d'une négligence, soit comme corollaire logique de l'autorisation donnée à l'utilisateur qui rendrait l'abonné mandant d'actes passés (par les membres de sa famille)... »

« Professionnel, le banquier répond de sa technique, il en répond, c'est-à-dire qu'il en est responsable, il en assume le risque... » (75).

Cette solution paraît raisonnable même si le face à face de deux professionnels, la banque et l'entreprise, laisse plus de place à la discussion (76) que dans le cas des systèmes axés sur le consommateur (tel en Belgique Mister Cash, Bancontact...) où l'inégalité dans l'accès à l'informatique justifie que l'on fasse supporter le risque de défaillance par la banque.

2) *Deux remarques pratiques* compléteront ces observations de principe :

a) La charge de la preuve détermine qui, en fait, supporte le risque de défaillance du système. Il est tout aussi difficile pour une banque de prouver que le transfert irrégulier est dû à la négligence du client, qu'à ce dernier de prouver qu'une banque a conçu un système de sécurité inapproprié ou n'a pas respecté ses propres procédures de sécurité.

Les contrats règlent soigneusement la charge de la preuve en prévoyant, par exemple, que le journal des transactions effectuées (le « *logging* »), établi par la banque, constitue une preuve formelle et suffisante des ordres donnés par l'abonné, et ce, quel qu'en soit le montant.

Le système fonctionne de la façon suivante : le *logging* issu de l'ordinateur de la banque, est supposé (présomption réfragable) reprendre fidèlement les instructions du client. Celui-ci est responsable pour l'ordre qui émane de ses locaux jusqu'à l'ordinateur de la banque.

Des extraits de compte sont également remis au client, soit sous forme classique, soit par télématique. Il a la possibilité de les contester la banque étant responsable de la distorsion existant, le cas échéant, entre les instructions reprises par le *logging* et les mentions portées sur l'extrait de compte.

b) Il ne faudrait pas conclure de l'exposé sommaire présenté ci-dessus que les cas de fraude ou d'erreur sont légion. Ils sont en réalité marginaux (même s'ils peuvent avoir des conséquences financières très importantes) parce que les banques essaient d'en prévenir l'occurrence par des mesures de sécurité comportant notamment le changement des mots de passe, la liste des personnes autorisées à initier le paiement, la liste des bénéficiaires autorisés.

(75) M. Vasseur, art. cité p. 592 ; sur la répartition des responsabilités dans les systèmes grand-public, D. Syx, Aspects juridiques du mouvement électronique de fonds, Kredietbank, 1982, p. 30 et s.

(76) Cfr à ce sujet les hésitations significatives de la jurisprudence française sur la présomption de connaissances des vices cachés pesant sur le vendeur professionnel lorsque celui-ci traite également avec un acheteur professionnel, mais dans une spécialité différente, cfr. aussi la solution prônée par D. Carton pour le télex dans son article, Aspects juridiques des ordres de virement transmis par télex, D.I.S.E.P., n° 2, octobre 1985, p. 3 et s.

Si l'on en croit certains responsables financiers dans les entreprises la complexité même des procédures de sécurité (exemple mot de passe) serait un obstacle à la diffusion des systèmes de transfert électronique de fonds. Y aurait-il antinomie entre l'exigence de *rapidité* inhérente à la vie des affaires et la relative lourdeur des procédures destinées à assurer la sécurité du système ?

3) Si les contrats examinés visent spécifiquement le cas de la fraude, leurs dispositions permettent aussi de régler en pratique l'hypothèse de l'erreur.

— Selon les principes, la banque est responsable de l'erreur qu'elle commet dans l'exécution d'un ordre correct donné par le client (77). A cet égard, les contrats font obligation au client de contester les mentions des relevés périodiques qui lui sont adressés. A défaut, il est présumé marquer son accord sur ces mentions et donc sur la façon dont les instructions ont été exécutées par la banque.

— Il n'est pas exclu que le client commette une erreur dans les instructions données à la banque. Il sera tenu, en principe, des conséquences de cette erreur (78).

B3. — *REVOCATION D'UN ORDRE DE TRANSFERT : CONDITIONS.*

Le client qui donne un ordre de transfert erroné, ou qui est la victime d'un ordre de transfert frauduleux, perd-il tout espoir de recouvrer le montant transféré ? (79).

En principe, non. Il pourra, en effet, actionner le bénéficiaire pour enrichissement sans cause ou, s'il y a fraude, pour complicité dans un

(77) Voir à propos des virements Bruyneel, op.cit., p. 423.

(78) Voir à propos des virements et pour plus de détails Van Ryn et Heenen, op. cit., n° 2063, 4e - Bruyneel op.cit., p. 430.

(79) A ce sujet, J.-P. Spreutels, Virement par erreur et cel frauduleux, R.C.J.B. 1984, p. 35.

détournement de fonds (80). La prévention est cependant préférable, car le bénéficiaire peut être devenu insolvable et le client supporte ici la charge de cette insolvabilité.

Il est donc de l'intérêt du transférant si la banque n'a pu déceler la fraude ou l'erreur, d'annuler, ou plutôt de révoquer, l'ordre de transfert de fonds émis.

Ceci suppose cependant que le contrat liant le donneur d'ordre à sa banque n'interdise pas une telle révocation et que le transfert de fonds n'est pas achevé (pour plus de détails sur la notion de paiement définitif voir *infra*).

Si le donneur d'ordre a révoqué à temps et dans les formes son ordre de transfert, il est en droit d'exiger que sa banque prenne les mesures appropriées pour éviter que l'ordre de transfert frauduleux ou erroné ne produise ses effets ou ne les poursuive (81).

Si la banque exécute l'ordre de transfert, elle sera tenue du dommage qui en découle car l'opposition ou la révocation coupe, à notre avis, le lien de causalité entre l'erreur du client ou la fraude et le dommage subséquent (82).

C. — *LA BANQUE DU TRANSFERANT : RESPONSABILITE POUR TOUT LE RESEAU ?*

Qu'il s'agisse de transferts réguliers exécutés tardivement ou de transferts irréguliers, un problème très délicat surgit quand l'inexécution de l'ordre n'est pas le fait (au sens matériel) de la banque du donneur d'ordre (ou banque transférante), mais celui d'une banque correspondante ou intermédiaire (83) dont le concours est nécessaire pour assurer l'acheminement du transfert.

Deux questions se posent.

1° La banque du donneur d'ordre qui se substitue une banque correspondante pour l'exécution de sa mission contractuelle, doit-elle répondre vis-à-vis du donneur d'ordre, des fautes commises par la banque correspondante ?

La réponse est positive car les fautes commises par l'agent d'exécution ne constituent pas pour le débiteur une cause étrangère. Le cocontractant est tenu de l'exécution de ses obligations, même s'il s'adjoint les services d'un correspondant à cet effet (84).

L'application pratique de ce principe pose cependant des problèmes.

Le cas où le correspondant de la banque transférante tombe en faillite, rendant par là impossible l'exécution de l'ordre, est difficile à traiter au regard des règles classiques de la responsabilité car la faillite est un événement souvent imprévisible et indépendant de la volonté de la banque transférante (banque du donneur d'ordre).

On peut songer à lui imputer le dommage sur base d'une faute dans le choix de ses correspondants mais force est de reconnaître que c'est plus la théorie du risque que celle de la faute qui est sous-jacente à cette solution.

Un autre cas difficile à trancher est celui où le donneur d'ordre a marqué son accord sur les étapes du transfert, ce qui rend moins crédible le reproche fait à la banque transférante d'une faute dans le choix des moyens pour opérer le transfert même si ceux-ci sont proposés par la banque transférante sans doute mieux informée que son client sur la qualité des institutions financières.

Plus fondamentalement, le donneur d'ordre pourrait être privé de recours contre sa banque *parce que cette dernière a pris la précaution de s'exonérer de la responsabilité pour les fautes commises par son agent d'exécution, en l'occurrence une banque correspondante.* D'où la seconde question :

2° Le donneur d'ordre, qui est un tiers par rapport au contrat passé entre sa banque et la banque correspondante, peut-il exercer un recours contre la banque correspondante et quelle est la nature de ce recours ?

La réponse est à chercher dans l'article 1165 du Code Civil qui interdit à un tiers, en principe, de puiser un droit dans une convention à laquelle il n'est pas partie et qui consacre l'indépendance des contrats, même si des liens les regroupent. Il ne faudrait pas en déduire hâtivement que le donneur d'ordre est totalement démuni de recours contractuel contre la banque intermédiaire.

(80) Les considérations développées au texte s'appliquent mutatis mutandis à la banque victime d'une fraude ou d'une erreur.

(81) La rapidité et l'automatisation inhérentes aux transferts électroniques de fonds rendent en pratique la révocation plus malaisée.

(82) Pour plus de détails D. Syx, op. cit., p. 32 et s. B. Amory et X. Thunis, note sous Trib. Comm. Liège, 19 janvier 1984, in La télématique, Aspects techniques, juridiques et socio-politiques, Story Scientia, 1984, p. 281 et s.

(83) A l'exclusion de la banque du bénéficiaire, voir supra.
Pour plus de détails sur cette question, P. Van Ommeslaghe R.C.J.B. 1986, spécialement p. 212 et s.

(84) Un arrêt de la Cour de cassation du 21 juin 1979 (J.T. 1979 p. 675) applique la solution à la matière des virements.

La doctrine dominante (85) considère en matière de virement — et ceci est à notre avis transposable aux transferts électroniques — qu'un mandat existe dans les rapports entre le donneur d'ordre et sa banque qui demande, au nom et pour le compte de celui-ci, de créditer le compte du bénéficiaire. Si une banque intermédiaire intervient dans le circuit, c'est en qualité de mandataire substitué de la première banque (86). Toute cette construction suppose naturellement que le paiement est un acte juridique puisque le mandat porte sur l'accomplissement d'actes juridiques.

L'intérêt essentiel est de conférer au donneur d'ordre, sur base de l'article 1994 du Code Civil, une action directe contre la banque intermédiaire (87) (88).

Ce n'est pas ici le lieu d'entrer dans une discussion approfondie sur la qualification du virement qui, soulignons-le, est inhérent à un dépôt de fonds ou à l'octroi d'un crédit. Il s'agit d'un service gravitant autour de la notion de compte et cet aspect de service apparaît de façon particulièrement nette dans les contrats passés entre la banque et le client par lesquels la première offre au second un mode supplémentaire — électronique — de mobilisation des fonds déposés ou du crédit octroyé. La variété et l'importance des prestations d'ordre *matériel* que la banque s'engage à exécuter pour l'entreprise cliente évoquent plus semble-t-il, le louage d'ouvrage que le mandat.

La qualification de louage d'ouvrage n'est pas favorable au donneur d'ordre sur le plan pratique, car par le jeu de l'art. 1165 du Code Civil, celui-ci se voit privé de tout recours contractuel direct contre la banque correspondante sauf à considérer ce qui est une explication doctrinale quelque peu incertaine, que le donneur d'ordre est bénéficiaire d'une stipulation pour autrui greffée sur le contrat passé entre les banques.

Une solution reste alors ouverte au donneur d'ordre pour obtenir une réparation du préjudice : intenter une action en responsabilité

(85) Cette doctrine est cependant loin d'être uniforme. On lira avec intérêt les divergences de vues entre A. Bruyneel op. cit., p. 381 et 382 spécialement et Van Ryn et Heenen op. cit., n° 2064 sur la qualification du rapport existant entre la banque du donneur d'ordre et la banque du bénéficiaire.

(86) Cfr. en ce sens M. Cabrillac et J.L. Rives-Lange Encyclopédie Dalloz Dr. Comm. Vo virement n° 75 et s. ; en droit américain voir l'étude de D. Ambrosia, New S.W.I.F.T. rules on the liability of financial institutions for interest lones caused by delay in international fund transfers, Cornell Int. Law Journal 1980 spéc. p. 316 et s.

(87) Elle a aussi son importance en ce qui concerne la révocation des ordres de transfert qui peut être demandée jusqu'à l'inscription au crédit du compte du bénéficiaire.

(88) Pour plus de détails, voir P.A. Foriers, observations sur l'article 1994 du Code Civil et l'action directe née de la substitution R.C.J.B. 1981 p. 469 et s. (critique de la notion d' «action directe »).

délictuelle (C.C. 1382) contre la banque fautive (89).

Cette solution n'est cependant pas totalement satisfaisante : elle est discutable sur le plan théorique (90) et elle aboutit en définitive à faire reposer le risque de l'opération sur le donneur d'ordre (exemple : le recours contre une banque insolvable) et, de façon plus générale, à lui faire supporter le risque d'un mode de transfert auquel il est extérieur. Que l'on songe au cas où le transfert n'a pas été effectué correctement et où il n'est pas possible, contrairement à l'hypothèse développée ci-dessus, de déterminer quelle est la cause du préjudice. Chaque entité du système va affirmer que le problème lui est étranger, avec toutes les difficultés de preuve que cela implique pour le client.

Cette difficulté d'identification peut amener à prôner, au moins *de lege ferenda*, la responsabilité pour l'ensemble de l'opération de la banque transférante, solution qui présente d'incontestables avantages pour l'utilisateur.

Dans le domaine du transport des marchandises par route, l'article 3 de la convention C.M.R. indique que « le transporteur répond... des actes et omissions de ses préposés et de toutes autres personnes aux services desquelles il recourt pour l'exécution du transport... »

Il s'agit là d'un précédent intéressant qui pourrait alimenter la réflexion pour d'éventuelles directives sur les transferts électroniques de fonds.

D. — *LES RELATIONS INTERBANCAIRES.*

Entre organismes bancaires les problèmes de responsabilité ne sont pas moins délicats à résoudre. Quand la responsabilité du traitement d'un ordre passe-t-elle d'une institution à l'autre ?

S.W.I.F.T. offre à cet égard un exemple intéressant de partage de

(89) La banque fautive pourrait-elle se prévaloir d'une clause limitative de responsabilité dont elle bénéficierait dans ses rapports avec la banque du donneur d'ordre ? La doctrine dominante soutient généralement que la convention limitative de responsabilité couvre aussi bien la responsabilité aquilienne que la responsabilité contractuelle (cf. par exemple Fagnart et Deneve, Responsabilité civile, chr. de jurisp. J.T. 1985, p. 457), mais la solution n'est-elle pas différente ici puisque le donneur d'ordre est un tiers par rapport au contrat et donc par rapport à la clause exonératoire.

(90) Un recours extra contractuel sera rarement possible en pratique, car la Cour de cassation belge considère que les agents d'exécution ne sont responsables envers les tiers que dans les cas de violation d'une obligation qui s'impose à tous et pour autant que cette faute ait causé un dommage autre que celui qui découle de la seule inexécution fautive du contrat (cfr. sur ce point, Fagnart et Deneve, ibid. ; Van Ommeslaghe R.C.J.B. 1985, op. cit. n° 102).

responsabilité (91) dont pourraient sans doute s'inspirer utilement d'autres réseaux télématiques (92).

S.W.I.F.T. est responsable en principe de l'exécution correcte des services que la société propose, en ce compris pour les mesures de sécurité (art. 7.1.).

S.W.I.F.T. garantit une intervention pour perte d'intérêts due à un paiement tardif dès lors qu'une faute peut lui être reprochée. Cependant S.W.I.F.T. n'est responsable que de la perte ou du dommage direct causé à un utilisateur ou à un membre ayant satisfait aux règles de procédure prévues et dans les limites fixées par le manuel (art. 7.2.2.)

Un plafond est fixé à la responsabilité : un milliard de francs belges en cas d'actes frauduleux d'employés de S.W.I.F.T. et 400 millions de francs belges en cas d'erreur ou d'omission. S.W.I.F.T. n'est pas responsable pour des transferts frauduleux émis par un tiers étranger au personnel S.W.I.F.T.

Il est à noter que S.W.I.F.T. limite sa responsabilité au dommage direct, c'est-à-dire à la perte en capital qui fait l'objet du message ainsi qu'aux pertes d'intérêts parfois improprement dénommées dommages indirects (consequential damages) (93).

La banque qui émet un message est en principe responsable jusqu'à la prise en charge par S.W.I.F.T. du message.

La banque destinataire est responsable en principe à partir de la transmission par S.W.I.F.T. du message.

Les participants sont responsables pour la correcte exécution des règles de forme et de la procédure, de même que pour un éventuel manque de diligence de leur part (94).

De façon plus générale, le professeur Scott (95) a proposé deux principes de base en cas de modification substantielle d'ordres pourtant

(91) Voir S.W.I.F.T., User Handbook Chapter 6 Bank responsability et Chapter 7, S.W.I.F.T. Responsability and Liability.
Le règlement du C.E.C. (Centre d'échange d'opérations à compenser du système financier belge) comporte également quelques dispositions intéressantes en cas de défaillance d'un des membres (art. 83 et s.). Cfr. aussi les dispositions concernant le règlement des responsabilités (notamment art. 106 et s.). Pour plus de détails A. Bruyneel, op. cit., p. 374 et s.

(92) Le résumé qui suit est repris de E. de Lhoneux, Télématique et droit monétaire, In La Télématique, t. II, Aspects techniques, juridiques et socio politiques, Story Scientia 1984, Colloque organisé à Namur, p. 285 et s.

(93) Voir S.W.I.F.T. User Handbook Chapter 7.

(94) Pour plus de détails sur l'allocation des responsabilités dans S.W.I.F.T., cfr. H. Lingl, Risk Allocation in International E.F.T., Chips & S.W.I.F.T., HLR 1981, n 3, p. 638 et s.

(95) H. Scott, art. cit. p. 980.

régulièrement donnés par le donneur d'ordre, mais ayant fait l'objet d'un traitement erroné ou frauduleux de la part d'un opérateur ou même d'un étranger au système :

1) L'organisme transmetteur, la banque intermédiaire ou destinataire, sont responsables de tout dommage occasionné par toute modification qu'ils ont apportée à l'ordre.

2) La première banque à effectuer un paiement sur la base d'un ordre modifié substantiellement par un tiers est responsable du préjudice qui en résulte.

La seconde règle s'affranchit manifestement du concept de faute pour mettre à charge de la banque les *risques* de fraude commise par des tiers étrangers.

Ces règles sont tirées d'un Code uniforme des nouveaux moyens de paiement proposé par le professeur Scott récemment discuté aux Etats-Unis. Il semble d'ailleurs que l'utilité et les dispositions de base en soient contestées.

IV. — LE MOMENT DU TRANSFERT.

A. — *IMPORTANCE DE LA QUESTION.*

On sait qu'en droit civil, le paiement consiste dans l'exécution, par le débiteur, de l'obligation contractée à l'égard de son créancier. Ainsi, en matière de virement, le paiement n'est effectué qu'au moment où le compte du créancier est crédité (96).

On pourrait a priori penser que le transfert électronique de fonds simplifie la question de la détermination du moment du paiement puisqu'il rapproche, par sa rapidité d'exécution les moments où l'ordre de débit est donné et celui où le compte du créancier est crédité, ce qui diminue aussi, d'ailleurs, les possibilités de révoquer les ordres de transfert. Le problème demeure épineux vu la pluralité d'intervenants. Il est cependant important à plusieurs égards :

— le moment du paiement sert de référence pour déterminer si les fonds ont atteint leur destinataire dans un délai spécifié contractuellement,

(96) La jurisprudence relative à la faillite fourmille de difficultés relatives au moment, antérieur ou postérieur à la déclaration de faillite, où le paiement initié par virement est complet, cfr. à ce sujet P. Coppens et F. t'Kint, 1984, p. 508, n 73.

— le moment du paiement intervient également quand une banque ou un client transfère par erreur des fonds à une autre banque qui tombe en faillite (ou dont le client tombe en faillite) (97). Si la banque faillie (ou son client) n'était pas le destinataire du paiement, mais que celui-ci est définitif, celui qui a initié le paiement indû sera créancier de dividendes dans la masse du failli au lieu de prétendre à la récupération du principal
Autre exemple : un conflit peut surgir entre un tiers revendiquant (exemple : un curateur) et le créancier du donneur d'ordre (tombé en faillite), qui, bénéficiant d'un ordre de transfert, soutient que le droit du tiers sur le compte du donneur d'ordre est né après l'exécution complète du transfert.

— la détermination du moment du paiement permet aussi d'évaluer le retard par une institution financière à exécuter un ordre de crédit (98).

B. — *QUAND UN TRANSFERT ELECTRONIQUE DE FONDS DEVIENT-IL DEFINITIF (99) ?*

Nombre de critères ou de moments peuvent être pris en considération pour déterminer quand un transfert de fonds est définitif :

1° Le moment où le compte du donneur d'ordre est débité. Le fondement théorique de cette solution est à chercher dans la dépossession des fonds que le donneur d'ordre encourt suite à l'ordre de transfert. Néanmoins, quand une banque intermédiaire s'interpose entre la banque du donneur d'ordre et celle du destinataire, la banque intermédiaire pourrait être considérée comme un mandataire de la première banque. Le transfert ne sera considéré comme définitif que lorsque le compte de la banque intermédiaire aura été débité (100).

Beaucoup de systèmes bancaires, cependant, confortés par la jurisprudence anglo-saxonne, ne reconnaissent un caractère définitif au transfert que lorsque la banque destinataire, d'une façon ou d'une autre, a été impliquée dans le processus de transfert (2° à 6° ci-dessous). Ainsi ont été évoqués comme pouvant constituer le moment où le transfert devient définitif :

(97) Voir à ce sujet, Ann Arora, Recent developments in money transfer methods Lloyds Maritime and Commercial Law, 1980, p. 429.

(98) Pour plus de détails, D. Ambrosia, New S.W.I.F.T. rules on the liability of financial institutions for interest losses caused by delay in international fund transfers, Cornell Int. Law Journal, 1980, p. 318.

(99) Pour plus de détails, voir l'étude très complète réalisée sous l'husnice des Nations-Unies, Draft Legal Guide on Electronic Funds Transfers, 30 april 1985, A/CN9/266/Add. 1.
Pour une discussion en matière de virement, voir A. Bruyneel, op. cit., p. 400 et s.

(100) Sur cette questiun, v. Rev. Trim. Dr. Comm. 1984, p. 129 et s.

2° Le moment où le compte de la *banque* destinataire est crédité.

3° Le moment où la *banque* destinataire est avertie qne le montant du transfert est porté à son compte.

4° Le moment où la *banque* destinataire accepte le transfert porté à son compte.

5° Le moment où le transfert est porté au *compte du bénéficiaire*.

6° Le moment où le *bénéficiaire* est averti que le montant du transfert est porté à son compte.

7° Le moment de la *compensation* entre les banques. Cette dernière solution paraît avoir la faveur des praticiens.

C. *APPRECIATION.*

Il n'est pas possible d'examiner ici en détail les solutions proposées dont certaines ont été retenues par une jurisprndence anglo-saxonne hésitante dont l'analyse sort du cadre de nos recherches.

Certaines de ces solutions, même correctes en principe, posent des problèmes pratiques. Ainsi, dans la quatrième solntion, il peut être difficile de déterminer avec précision le moment de l'acceptation si les formes n'ont pas été préalablement établies.

A notre avis, un critère à prendre en considération pour déterminer si un transfert est définitif, est la mise à disposition, non susceptible de remise en question, *non précaire* (au sens où l'entend le droit des biens) des fonds faisant l'objet du transfert (101).

Il ressort en effet de la pratique bancaire internationale que souvent la banque destinataire procède au crédit du compte de son client « sous réserve de bonne fin », c'est-à-dire sous réserve d'un règlement ultérieur par la banque située en amont.

Le transfert de fonds n'est donc définitif que lorsque le crédit est irrévocable.

De façon générale, la matière semble assez confnse et il serait utile que l'accord se fasse clairement sur les concepts fondamentaux et leur mise en œuvre pratiqne. Le règlement de S.W.I.F.T. constitue un effort en ce sens (102).

(101) Cfr. en ce sens, Recommandation n° 4 du projet de résolution du Comité de droit monétaire : « Est seul décisif le moment à partir duquel le créancier dispose contre sa banque d'une créance inconditionnelle et irrévocable issue de la bonification sur son compte... »

(102) Voir notamment les articles 6.4.3.2. et 6.4.3.3. du S.W.I.F.T. User Handbook, définissant les concepts de pay date et de value date.

EN CONCLUSION . . .

Pour excitante qu'elle soit, la complexité des problèmes juridiques abordés dans ce rapport ne doit pas nous détourner de réflexions plus fondamentales qui s'inscrivent d'ailleurs dans le droit fil des préoccupations des organisateurs de ce colloque.

1) Bien que le juriste ait une propension à mettre en évidence les hypothèses conflictuelles, on constate que les conditions de production de celles-ci ont, jusqu'ici, été rarement réunies comme l'atteste, en Europe continentale tout au moins, une jurisprudence peu abondante. Sans doute faut-il expliquer cette discrétion relative par deux facteurs principaux :

1° Une technologie assez sûre qui réduit les sources de conflit.

2° La qualité des parties à l'opération télématique : il s'agit de professionnels soucieux de *régler* les conflits de façon non contentieuse et, aussi, de les *prévenir* par une technique sans cesse plus fiable et par des normes auto-régulatrices empruntant des voies « informelles » (normes techniques, contrats d'adhésion, conventions inter-bancaires).

2) Face à une évolution technologique galopante, le juriste, armé de concepts vénérables, semble démuni. La tentation est forte de crier au bouleversement et d'appeler à une « révolution juridique ». Notre droit privé, qui s'est constitué à une époque où la valeur économique semblait indissociable d'une production matérielle, ne répond pas, il est vrai, à toutes les questions que suscitent les techniques de traitement et de transport de l'information. Est-ce à dire qu'une réforme législative d'envergure s'impose ? A notre avis, la réponse est actuellement négative.

Sans doute un aménagement du droit de la preuve s'impose-t-il comme l'attestent la loi française du 1er juillet 1980 et le récent projet de loi luxembourgeois. Dans ce domaine, le législateur devrait, à notre avis, avoir pour souci de lier le moins possible les définitions et l'application d'une nouvelle législation aux supports techniques existants.

On pourrait aussi affirmer plus nettement le principe de la responsabilité de la banque transférante (voir *supra)* et définir plus précisément les limites du temps dans lesquelles doit normalement être exécuté un transfert électronique de fonds, ainsi que le moment où le transfert de fonds devient définitif.

L'évolution technique dont les résultats et les progrès précisent par touches successives le véritable rôle et la véritable utilité du droit est loin d'être achevée. Voulant tout régir, une forme législative risque d'être tatillonne. Voulant régir tout de suite, elle risque d'être rapidement obsolète.

D'aucuns ont, à juste titre, parlé d'un « droit en attente » (103). L'expression ne réfère pas à un prétendu vide juridique, car dans cette matière qui s'accommode mal de particularismes locaux, les milieux professionnels, utilisant les possibilités offertes par la liberté contractuelle, secrètent, aux plans national et international, des pratiques autorégulatrices dont une expression anglaise, difficilement traduisible, « *soft law* » (droit assourdi, droit vert) évoque la souplesse d'adaptation (104).

Par ailleurs, parler d'un vide juridique c'est oublier le secours que nous apportent, dans des matières très techniques, la « relecture » des principes fondamentaux, l'approfondissement des classifications, l'affinement des concepts de base, dont on tire la solution de questions juridiques complexes. Ramener, autant que faire se peut, des situations nouvelles à des règles existantes, c'est là travail de juriste.

(103) De Lhneux, op. cit., p.288.

(104) Rappelons que les présents développements s'appliquent à la télématique professionnelle.