Université Robert Schuman
Strasbourg III

ORDRE DE PAIEMENT SUR INTERNET

Katerina Hendrychova

2001

D.E.A. Droit des affaires

Sous la direction de

M. le Professeur Théo Hassler

M. le Professeur Michel Storck

Sommaire

Liste des abréviations

Bull. civ.	*Bulletin des arrêts de la Cour de cassation (chambres civiles)*
CA	Cour d'appel
Cass. com.	Cour de cassation, chambre commerciale
ch.	Chambre
Chron.	Chronique
CNIL	Commission nationale de l'informatique et des libertés
CNUDCI	Commission des Nations Unies pour le droit commercial international
CVD	Carte virtuelle dynamique
DIT	*Droit de l'informatique & des télécoms*
E-Sign	Electonic Signature in Global and Nation Commerce Act
ibid.	Au même endroit
ICP	Infrastructure à clé publique
IR	Informations rapides
JCP	*Juris-Classeur périodique*
- éd. E	- édition Entreprise
- éd. G	- édition générale
JOCE	Journal officiel des Communautés européennes
JT	*Journal des tribunaux*
obs.	Observation
p.	Page
PKI	Public Key Infrastructure
Rev. dr. bancaire	*Revue de droit bancaire et de la bourse*
RDBF	*Revue de droit bancaire et financier*
RIDC	*Revue internationale de droit comparé*
RJC	*Revue de jurisprudence commerciale*
RTD com.	*Revue trimestrielle de droit commercial*
s.	Et suivantes
Somm.	Sommaires
SPA	Secure Payment Application
T. corr.	Tribunal correctionel
TCP/IP	Transport Control Protocol /Internet Protocol
TILA	Truth in Lending Act
UETA	Uniform Electronic Transaction Act

Introduction

1 Louées par les uns et damnées par les autres, les nouvelles technologies de l'information envahissent la vie quotidienne. Elles s'intègrent dans les relations sociales et font ainsi naître la société de l'information.

2 Le droit a vocation de réglementer la conduite des hommes, il est l'instrument d'un certain équilibre des relations sociales. En conséquence, il s'applique nécessairement à la réalité façonnée par les nouvelles technologies de l'information.

3 Le bouleversement informatique est un phénomène relativement récent et en pleine évolution. Par contre, le rôle normatif du droit implique l'exigence de stabilité. Certainement, le droit n'est pas insensible à la réalité qui l'entoure. Mais il ne réagit qu'*a posteriori*.

Dans le sens inverse, le droit a la force d'influencer les relations sociales. En effet, celles-ci doivent se conformer aux exigences du droit. Le droit a le pouvoir d'orienter l'évolution des relations sociales. Ainsi, le droit peut agir positivement ou négativement sur le développement de la société de l'information qui se caractérise par la place centrale qu'occupe l'information et les technologies servant à la produire, l'exploiter ou la communiquer[1].

4 Internet représente une manifestation importante de la société de l'information. Il constitue un réseau des nouvelles technologies de l'information.

Internet a son origine dans le réseau Arpanet, un réseau expérimental destiné à permettre le transfert de fichiers entre les gros ordinateurs de centres de recherche militaire américains[2]. L'idée de cet ancêtre d'Internet est née en 1957, à la suite du succès soviétique dans le domaine spatiale dû au lancement du premier satellite artificiel de la Terre. Pour prévenir les atteintes contre la sécurité nationale américaine, Arpanet est conçu comme un réseau « sans tête » qui pourrait s'adapter à n'importe quel type d'ordinateur utilisé. En 1974, le protocole TCP/IP[3] a vu le jour. Dorénavant, l'interconnexion de réseaux hétérogènes à différents débits est possible.

---

[1] D. KAPLAN, « La France dans la société de l'information », mai 2001, disponible sur http://www.premier-ministre.gouv.fr/fr/p.cfm?ref=25274#1 .
[2] http://encyclo.voila.fr/ , mot-clé « Internet ».
[3] Transport Control Protocol /Internet Protocol.

En 1979, le réseau Arpanet devient utilisable par les chercheurs civils. Dès l'année 1988, déjà sous le nom d'Internet, il devient mondial. Son développement ultérieur doit beaucoup à l'invention par Tim Berners-Lee du concept du World Wide Web. Celle-ci survient en 1991. Elle a permis de relier les informations diffusées sur Internet entre elles par des liens hypertextes et a alors introduit une présentation normalisée de l'information[4].

5 Ainsi est crée un réseau qui permet une communication rapide à distance. Aujourd'hui, les documents textuels, les images et les sons sont diffusés sur Internet. Pourtant toute cette communication est immatérielle ; les données circulent sous forme de bits.

Par l'emploi du protocole TCP/IP sus-mentionné, Internet a été empreint du caractère ouvert. Cela a facilité son utilisation internationale qui lui est dès lors propre.

6 Par ses caractéristiques, le réseau Internet est propice au commerce. Le commerce sur Internet fait partie des activités qui sont souvent désignées comme commerce électronique[5]. Différentes approches de cette notion existent. La première approche envisageable est basée sur une définition large. Il s'agit de « toute activité d'échange générant de la valeur pour l'entreprise, ses fournisseurs ou ses clients, effectuée sur des réseaux »[6]. Une deuxième définition, restreinte, est possible. Celle-ci couvre l'ensemble des activités commerciales conduisant à des transactions amorcées en ligne. Dans ce cas-là, l'opération de paiement liée à la transaction ne doit pas nécessairement se faire en ligne. Par contre, une troisième approche, étroite, ne considère comme commerce électronique que les transactions engagées et conclues en ligne, paiement compris.

7 Nous remarquons que suivant la définition retenue, l'opération de paiement en ligne doit ou ne doit pas être présente en commerce électronique. En pratique, un certain nombre d'opérations commerciales sont préparées sur Internet, or elles ne sont pas accompagnées du paiement sur Internet. Si la livraison du bien ou la prestation d'un service n'est pas instantanée, le défaut de paiement sur Internet peut être acceptable pour le commerçant et les modes de paiement hors ligne peuvent suffire. Or, lorsque le commerçant doit exécuter ses obligations nées du contrat conclu sur Internet immédiatement, il est de mise que l'acceptation de son offre par le cocontractant sur Internet et l'opération de paiement soient liées. C'est pour cette raison que les systèmes de paiement sur Internet sont recherchés.

8 Avant d'analyser les différents systèmes de paiement sur Internet, il est important de s'arrêter sur la notion de paiement. En effet, le terme de paiement peut avoir deux sens, un sens juridique et un sens économique[7]. Le paiement, tel qu'il est appréhendé par le Code civil aux articles 1235 et suivants, désigne l'exécution d'une obligation quelconque par laquelle le créancier obtient satisfaction et l'obligation est éteinte. Le paiement a ici un

---

[4] Rapport d'information de M. Jean-Pierre BRARD du 11 juillet 2001, n° 3229, disponible sur www.assemblee-nationale.fr .

[5] Le commerce électronique peut être effectué par de nombreux autres réseaux, tels que le Minitel ou les échanges des données informatisées (EDI). Pour plus de précisions, voir le Rapport d'information précité.

[6] Rapport précité.

[7] C. LUCAS de LEYSSAC et X. LACAZE, « Le paiement en ligne », *Communication – Commerce Électronique*, fév. 2001, Chron., p. 14.

sens plus général que dans le langage courant[8]. Par contre, le paiement au sens économique du terme constitue un mécanisme qui permet au *solvens* de faire parvenir à l'*accipiens* une somme d'argent[9]. Nous constatons que sous cette acception, le résultat consistant en une remise effective de la somme d'argent n'est pas l'élément nécessaire de la notion. Dans ce sens, le paiement est présent dans le terme de moyen de paiement de l'article L. 311-3 du Code monétaire et financier. Nous employons la notion dans ce sens économique lorsque nous parlons du paiement sur Internet.

9 Comme nous venons de l'évoquer plus haut, le paiement sur Internet ne caractérise pas le commerce sur Internet, ce dernier peut se contenter des autres modes de paiement. Tel n'est pas le cas de la commercialisation des biens numériques ou des services sur Internet[10]. Par le téléchargement d'un logiciel sur Internet, l'obligation du commerçant de livrer le bien est éteinte. De même, l'éditeur d'un journal payant sur Internet est libéré s'il permet l'accès aux articles. Pour ces situations et d'autres encore, le paiement sur Internet est une nécessité. Dans le domaine de la presse sur Internet, la migration vers un système d'accès payant à certaines pages s'impose suite à la crise du secteur publicitaire depuis le second semestre 2000 et la chute subséquente des recettes issues des annonceurs[11].

10 Vu la relative nouveauté du réseau Internet, les systèmes de paiement sur Internet sont toujours en pleine évolution. Le paysage des solutions de paiement sur Internet change constamment, c'est la course aux standards qui n'existent pas encore aujourd'hui mais devront nécessairement se fixer[12].

L'histoire du développement des systèmes de paiement sur Internet commence en 1992, lorsque le World Wide Web devient un succès[13]. Durant la première étape, des numéros d'identification des cartes de paiement ou des numéros de comptes bancaires circulent sur Internet sans aucunes précautions de sécurité. Jusqu'à nos jours, cette habitude n'est pas définitivement enrayée, bien que différentes alternatives sécurisées soient apparues. L'année 1994 a été particulièrement marquante. La société Netscape a développé le protocole SSL (Secure Socket Layer) qui a permis le transfert sécurisé des données sur Internet. Le « cyberbuck » de DigiCash, la première monnaie électronique, a vu le jour. Toujours la même année, deux start-ups, First Virtual Holding et CyberCash, sont entrés sur le marché. Le secteur bancaire n'a pas suivi la tendance innovante de création de nouveau systèmes de paiement. Mais ce retard a été rattrapé dès 1995, quand

---

[8] F. TERRÉ, P. SIMLER, Y. LEQUETTE, « Droit civil, Les obligations », 7e éd., Dalloz 1999, n° 1218, p. 1101.
[9] C. LUCAS de LEYSSAC et X. LACAZE, article précité, p. 14.
[10] Par leur dématérialisation, les biens numériques s'approchent des services car ils n'engendrent aucune livraison physique. Ainsi, dans le domaine de la fiscalité indirecte du commerce électronique, les biens numériques entrent dans le régime appliqué aux services.
[11] P. BORIES, « Internet payant : nécessités et réalités », *JDNet*, le 29 juin 2001, http://solutions.journaldunet.com/0106/010629intro_dossier_payant.shtml/ .
[12] Nous entendons par systèmes de paiement sur Internet les mécanismes par lesquels les fonds sont transférés du *solvens* à l'*accipiens* et où au moins le déclenchement du processus a lieu sur Internet. Les solutions de paiement sur Internet désignent les applications commerciales concrètes de ces systèmes.
[13] K. BÖHLE, « The Potential of Server-based Internet Payment Systems, An attempt to assess the future of Internet payments », Background Paper n° 3, *e*PSO, mars 2001, disponible sur http://epso.jrc.es/ .

une nouvelle phase du développement des systèmes de paiement sur Internet a débuté.

Pour sécuriser d'avantage le paiement par carte sur Internet, le protocole SET (Secure Eletronic Transaction) a été conçu en 1996 par les sociétés de cartes Visa International et MasterCard, permettant d'authentifier tous les acteurs du processus de paiement. Les initiatives visant à réglementer l'activité concernant la monnaie électronique sont apparues. Cette étape se termine par la disparition de la première génération des systèmes de paiement sur Internet. En 1998, le service de First Virtual a été arrêté et DigiCash a fait faillite.

La phase suivante, où nous nous trouvons actuellement, est marquée par la disparition des systèmes de paiement les plus innovants, notamment par le désaveu du système de la monnaie électronique. Les systèmes de paiement basés sur les comptes connaissent le succès. La nécessité de téléchargement d'un logiciel pour la mise en place du système de paiement par le consommateur est réduite au minimum. Elle est remplacée par l'accès à un serveur central qui peut même servir de plate-forme supportant différents systèmes de paiement. Instruits par l'évolution des systèmes précédents, les prestataires de paiement recherchent la simplicité et la sécurité des systèmes de paiement qu'ils mettent en œuvre sur Internet.

11 Si nous faisons un résumé de tous les systèmes de paiement qui sont ou ont été utilisés sur Internet, nous pouvons dresser une typologie fondée sur la distinction entre les systèmes de paiement basés sur les comptes et le système de la monnaie électronique.

Les systèmes de paiement basés sur les comptes peuvent être divisés d'après le caractère du compte en question. Les uns s'appuient sur les comptes bancaires, les autres sur les comptes non-bancaires. Dans les premiers systèmes cités, l'ordre de paiement peut être donné au moyen d'une carte de paiement, soit par l'envoi du numéro apparent d'identification de la carte, chiffré ou non, soit par le contrôle physique de la carte et de son code confidentiel. L'ordre de paiement peut aussi consister dans un simple ordre de virement à distance sur Internet dans le cadre du service de banque par Internet. Pour l'accès à ce service, un identifiant et un code confidentiel sont demandés. Les systèmes de paiement basé sur les comptes bancaires tendent alors à adopter au réseau Internet les moyens de paiement désignés traditionnellement à l'usage hors ligne.

Les systèmes de paiement fondés sur les comptes non-bancaires sont plus innovants. Ils mettent en place des comptes virtuels prépayés gérés par un prestataire de paiement sur Internet. L'argent ainsi collecté par l'intermédiaire est déposé sur un compte bancaire spécial au nom de l'intermédiaire et donc procure à ce dernier un crédit intéressant. L'ordre de paiement dans ce système s'apparente également à un ordre de virement. Nous devons remarquer qu'en vertu du Code monétaire et financier français, seuls les établissements de crédit peuvent recevoir des fonds du public et mettre à la disposition de la clientèle ou gérer les moyens de paiement. Ainsi, un prestataire de paiement sur Internet gérant les comptes virtuels doit obtenir l'agrément selon le livre V, titre I, chapitre 1, section 3 du Code monétaire et financier.

Le système de la monnaie électronique distingue entre les situations où les unités de valeur sont stockées sur la carte et les cas où le stockage est assuré par la mémoire

d'ordinateur. Dans le premier cas, le moyen de paiement utilisé pour le transfert des unités est appelé porte-monnaie électronique, dans l'autre le porte-monnaie virtuel. Les porte-monnaie électroniques ont plutôt vocation à être utilisés dans les points de vente réels. Le concept du porte-monnaie virtuel n'a pas connu de succès sur Internet.

La distinction entre les systèmes de paiement basés sur les comptes, bancaires ou non-bancaires, et le système de la monnaie électronique est d'importance fondamentale. Pour sa claire compréhension, nous devons expliquer au préalable quelques concepts élémentaires du droit bancaire.

12 Une somme d'argent est constituée d'un ensemble d'unités monétaires, unités de comptes idéales telles que franc ou euro. Ces unités monétaires sont incorporées dans un support dénommé l'instrument monétaire[14]. L'instrument monétaire, comme la monnaie fiduciaire (représentée par les pièces de monnaie et les billets de banque) ou la monnaie fiduciaire (désignant le solde des comptes), permet alors de stocker les unités monétaires.

Le transfert des unités monétaires est assuré par l'instrument de transfert d'unités monétaires. Le Code monétaire et financier français emploie dans ce contexte la notion de moyen de paiement.

La situation parfaitement claire se complique par le fait que les concepts susmentionnés se superposent dans certains cas. Ainsi, les pièces de monnaie et les billets de banque constituent à la fois l'instrument monétaire et le moyen de paiement.

Un autre facteur de complication existe encore. Parmi les moyens de paiement, il est important de distinguer entre ceux qui constituent les titres commerciaux, comme par exemple le chèque et ceux qui ont abandonné la technique les titres. Ces derniers moyens de paiement ne circulent pas, mais servent seulement à émettre les ordres de paiement. La plupart des systèmes de paiement sur Internet reposent justement sur ces moyens de paiement.

13 La distinction entre les systèmes de paiement basés sur les comptes et le système de la monnaie électronique prend sa source dans l'emploi de différents moyens de paiement par ces systèmes.

Le système de la monnaie électronique repose sur des moyens de paiement qui circulent. La nature juridique de la monnaie électronique a été débattue en doctrine. Aujourd'hui, il paraît être admis que la monnaie électronique ne constitue pas un nouvel instrument monétaire. Elle est analysée comme un titre de créance[15]. Par rapport aux systèmes de paiement basés sur les comptes, l'utilisation de la monnaie électronique libère le *solvens* dès l'instant de l'utilisation du moyen de paiement. Cela est justement dû à son caractère de titre qui transforme la simple créance du *solvens* sur celui qui détient ses fonds en un élément de valeur acceptable par l'*accipiens* comme la dation en paiement[16].

Par contre, les systèmes de paiement basés sur les comptes mettent en œuvre des

[14] Lamy Droit du financement, *Les instruments de monnaie électronique*, n° 2440, Éditions Lamy 2001.
[15] S. LANSKOY, « La nature juridique de la monnaie électronique », *Bulletin de la Banque de France*, n° 70, octobre 1999, p. 57.
[16] L'utilité de la titrisation tient dans le fait qu'elle fait naître la négociabilité de ce qui est incorporé dans le titre.

moyens de paiement qui ne circulent pas. À l'aide de ces derniers, le *solvens* émet un ordre de paiement à la suite duquel le détenteur de son compte est obligé de transférer les fonds par l'inscription de la somme au débit du compte du *solvens* et son inscription consécutive au crédit du compte de l'*accipiens*. Ainsi, le donneur d'ordre de paiement n'est libéré que lorsque la somme due est portée au crédit du compte de l'*accipiens*.

14 Le système de la monnaie électronique ne sera pas l'objet de notre étude. Nous devrons nous concentrer sur l'ordre de paiement sur Internet qui, dans ce système, est éclipsé par le transfert de créance.

Dans les systèmes de paiement sur Internet basés sur les comptes, l'ordre de paiement apparaît comme le pilier du processus de paiement. Il convient dès à présent d'analyser sa qualification juridique.

15 Incontestablement, l'ordre de paiement est un acte juridique[17]. Il s'agit d'une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique[18].

L'ordre de paiement est un acte juridique unilatéral. Nous soutenons cette qualification bien que le droit civil français n'a pas pour habitude de raisonner en utilisant cette catégorie. S'il est vrai que l'ordre de paiement entre dans un cadre contractuel préétabli entre le donneur d'ordre et l'établissement qui gère son compte, nous ne pouvons pas dire que l'ordre de paiement est un contrat car le consentement de l'établissement a été donné d'avance. Nous ne nions pas qu'un contrat peut ainsi se former. Mais l'ordre de paiement ne présente qu'une composante d'un tel contrat. La situation est semblable à celle de l'offre/la demande et du contrat : même si l'offre et la demande se rencontrent immédiatement pour former un contrat, ni l'offre, ni la demande ne sont un contrat en elles-même.

La réglementation lacunaire de l'acte unilatéral en droit civil français n'a pas permis d'élaborer une théorie générale propre à cette matière[19]. Alors, en l'absence de réglementation spécifique, il convient de transposer le régime juridique du contrat à l'acte juridique unilatéral.

16 Une qualification plus précise de l'ordre de paiement a été recherchée. Nous devons ici remarquer que cette qualification juridique varie selon les droits des différents États.

En doctrine française, l'ordre de paiement est le plus souvent considéré comme un mandat[20]. Or, certains auteurs considèrent que « les vertus explicatives du mandat sont limitées »[21]. Ils relèvent que le mandat laisse de côté l'extinction de la dette de restitution

---

[17] T. HASSLER, « La signature électronique ou la nouvelle frontière probatoire », *RJC* 2000, p. 196.
[18] *Vocabulaire juridique*, sous la direction de G. CORNU, Association Henri Capitant, Quadrige/Presses Universitaires de France, 2000.
[19] F. TERRÉ, P. SIMLER, Y. LEQUETTE, « Droit civil, Les obligations », 7e éd., Dalloz 1999, n° 46, p. 53.
[20] La même qualification est retenue en doctrine hellénique, néerlandaise, luxembourgeoise et portugaise. Par contre, la doctrine allemande, belge, espagnole et italienne se montrent enclines pour la qualification de délégation. Pour plus d'informations, voir R.-C. ÉCONOMIDES-APOSTOLIDIS, « La nature juridique des relations issues de l'utilisation d'une carte de crédit dans le droit des États membres dela C.E.E. », *RIDC* 1994, n° 4, p. 1025 et 1026.
[21] F. GRUA, « Sur les ordres de paiement en général », *DS* 1996, 20e cahier, Chron., p. 172.

de l'établissement teneur de compte envers le déposant. Ils proposent ainsi d'analyser l'ordre de paiement comme l'acte d'indication d'un tiers pour la remise des fonds en dépôt, prévu à l'article 1937 du Code civil. En effet, l'ordre de paiement combine le mandat, pour ce qui est de l'extinction de l'obligation du donneur d'ordre de paiement envers le commerçant, et l'indication d'un tiers, pour ce qui est de l'extinction de l'obligation de l'établissement teneur de compte envers le déposant – donneur d'ordre de paiement[22].

D. MARTIN a proposé, en analysant le règlement par carte de paiement, une autre qualification de l'ordre de paiement, à savoir acte translatif du droit de propriété sur la provision. Nous n'adhérons pas à cette position. D. MARTIN soutient que l'utilisation d'une carte de paiement pourrait investir le commerçant d'un titre de propriété monétaire. Il nous semble qu'aucun titre n'est présent. Si le titre peut être dématérialisé, il ne peut pas être inexistant. En plus, dans l'état actuel du droit, le déposant n'a pas le droit de propriété sur les sommes déposées. Dans tous les cas, même si le législateur, en instaurant l'irrévocabilité de l'ordre donné au moyen d'une carte, a rapproché le régime juridique de l'ordre de paiement par carte de celui d'un acte translatif de droit, les règles s'appliquant aux ordres de paiement donnés par d'autres moyens de paiement sont différentes.

17 L'ordre de paiement s'insère dans un cadre contractuel préétabli qui met en relation trois acteurs : le consommateur, l'émetteur du moyen de paiement et le commerçant. Ce cadre contractuel repose sur deux contrats-cadres, l'un conclu entre le consommateur et l'établissement émetteur et l'autre conclu entre l'établissement émetteur et le commerçant.

Dans notre étude, le terme de consommateur ne sera pas toujours à prendre dans le sens strictement juridique du terme. En général, nous employons la notion dans un sens économique, faute de terme générique adéquat désignant le donneur d'ordre potentiel.

18 Tout ce que nous venons d'exposer sur l'ordre de paiement en général est transposable à l'ordre de paiement sur Internet. Mais, de nouveaux problèmes surgissent en ligne.

Dans l'espace dématérialisé où la communication se fait à distance, la vérification de l'identité des personnes réelles est imprégnée de probabilité. Internet filtre la réalité. Il permet de dissocier les différents éléments de l'identité. S'il existe des procédés qui sont capables de détecter « l'identité » de l'appareil depuis lequel l'ordre de paiement a été envoyé dans le réseau, les procédés permettant d'unir l'identité virtuelle à l'identité réelle ne sont qu'au stade d'essais. Nous pensons ici à la biométrie, grâce à laquelle il serait possible de passer à l'identification à cent pour cent.

Le caractère ouvert d'Internet engendre le problème de la sécurité des données transmises par le réseau. Internet n'était pas développé pour l'échange des données confidentielles. Ainsi, des procédés spécifiques doivent être utilisés pour protéger le flux d'informations contenues, dans notre cas, dans l'ordre de paiement.

De part son caractère international, Internet provoque des confits de juridictions et de lois que le droit international privé a vocation à résoudre. Il est généralement admis que les questions concernant l'ordre de paiement sur Internet sont régies par le droit applicable au

[22] L. BERNET-ROLLANDE, « Principes de technique bancaire », Dunod 1997, p. 179.

contrat entre le consommateur et l'émetteur du moyen de paiement qui a servi pour ordonner le paiement.

19 Pour un bon fonctionnement d'un système de paiement, il est indispensable que l'ordre de paiement réponde aux attentes des acteurs du système de paiement.

Le consommateur a l'intention de s'acquitter de son obligation de payer le commerçant, sans exposer ses fonds déposés sur un compte à la fraude. Il recherche alors les solutions de paiement qui protégent les données permettant d'ordonner le paiement.

Pour le commerçant, le paiement représente une contre-prestation des biens ou des services qu'il fournit. Il recherche légitimement à avoir le paiement garanti. Dans les systèmes de paiement reposant sur les comptes, le paiement n'est jamais immédiat. Le client donne un ordre de paiement qui, subséquemment, déclenche le jeu des écritures en comptes. Cela veut dire que l'intérêt du commerçant désireux d'être payé doit s'orienter vers l'efficacité des ordres de paiement réguliers et la lutte contre la fraude dont il subit des risques.

De son côté, l'émetteur est aussi intéressé par la suppression d'ordres frauduleux dont la gestion peut s'avérer très coûteuse.

20 Pour rendre ces attentes effectives lors du paiement déclenché par l'ordre de paiement sur Internet, il est essentiel d'apporter les solutions aux difficultés sus-visées qui naissent en ligne.

Les solutions peuvent venir du domaine technique et du domaine juridique. Dans cette perspective, le juriste devra adopter une pensée techno-légale qui intègre les caractéristiques technologiques dans les solutions et les principes juridiques[23].

21 Sur l'exemple de l'ordre de paiement sur Internet, nous pourrons voir comment le droit réagit aux nouveaux problèmes pour lesquels il n'était pas construit. Le droit est-il capable, dans son état actuel, d'apporter des solutions adéquates ? Ne freine-t-il pas l'emploi des solutions techniques ? Que faut-il faire pour optimiser l'ordre de paiement sur Internet ? Nous essaierons de répondre à ces questions en comparant les approches de différents ordres juridiques et leurs effets sur la réalité technique.

22 L'ordre de paiement sur Internet est un acte d'importance capitale dans les systèmes de paiement en ligne. Il doit répondre à deux exigences fondamentales. Premièrement, l'ordre de paiement régulièrement donné doit aboutir sur le paiement. Deuxièmement, uniquement un ordre de paiement exempt de fraude doit aboutir sur le paiement.

Ainsi, dans la première partie de notre étude, nous serons amenés à examiner l'efficacité de l'ordre de paiement régulier sur Internet et dans la seconde partie, nous traiterons la suppression de l'ordre de paiement frauduleux sur Internet.

---

[23] S. DUSOLLIER et L. ROLIN-JACQUEMYNS, « Le défi du droit face au commerce électronique : les initiatives de l'Union Européenne », *Systèmes d'information et de management*, n° 1, Vol. 5, 2000, p. 2, disponible sur www.droit.fundp.ac.be/crid/eclip/default.htm .

PREMIERE PARTIE

L'efficacité de l'ordre de paiement régulier sur Internet

23 L'ordre de paiement est un acte juridique unilatéral. Pour qu'il puisse déboucher effectivement sur le paiement, il faut premièrement qu'il soit valide. À l'instar de l'article 1108 du Code civil français qui détermine les quatre conditions essentielles pour la validité des conventions, nous pouvons déduire que l'une des conditions essentielles pour la validité de l'ordre de paiement sera l'approbation de l'ordre par son auteur, c'est-à-dire son expression de volonté de procéder au paiement. C'est uniquement cette condition de validité qui retiendra notre attention, les trois conditions restant ne posant pas de problèmes spécifiques sur Internet.

24 L'approbation de l'ordre de paiement par son auteur doit s'extérioriser. Sur Internet, elle peut s'exprimer sous forme écrite[24]. L'approbation elle-même doit être valable, c'est-à-dire ne pas être donnée par erreur, ne pas être extorquée par violence ou surprise par dol[25]. Mais du point de vue d'un éventuel différend opposant la personne autorisée à disposer des fonds au commerçant ou à l'établissement de crédit, c'est la preuve de l'approbation de l'ordre de paiement par son auteur qui est importante pour l'efficacité de l'ordre. L'approbation de l'ordre de paiement doit être vérifiée. Cette démarche est essentielle pour la distinction entre les ordres de paiement valides et les situations où l'acteur prétendait utiliser les mêmes procédés techniques à des fins différentes.

25 Mais, la vérification de l'approbation de l'ordre de paiement est elle-même conditionnée par l'authentification de l'ordre de paiement. Lors que nous parlons de l'authentification de l'ordre de paiement[26], nous entendons par cela, d'une part, le processus de vérification de l'intégrité de l'ordre et, d'autre part, le processus de vérification de l'imputabilité de cet ordre à la personne désignée par l'ordre comme son auteur[27]. Si ces deux processus révèlent que l'ordre de paiement a pu être frauduleusement altéré ou qu'il ne peut pas être imputé à la personne qu'il désigne comme auteur, il serait

[24] Il s'agit de l'écrit tel que défini par l'article 1316 du Code civil français.
[25] L'article 1109 du Code civil français.
[26] Nous appliquons la définition de l'authentification des données d'après la normalisation internationale du vocabulaire de la cryptologie, ISO 8730. Il s'agit du « processus appliqué par l'expéditeur et le destinataire pour garantir l'intégrité des données et fournir l'authentification de l'origine des données ». L'intégrité des données est définie comme la « capacité qu'ont les données de ne pouvoir être altérées ou détruites d'une manière frauduleuse » et l'authentification de l'origine des données signifie la « confirmation que la source des données reçues est celle revendiquée ».
[27] Les termes d'intégrité et d'imputabilité sont empruntés à l'arrêt de la Chambre commerciale de la Cour de cassation du 2 décembre 1997, *Bull. civ.*, IV, n° 315, p. 271.

vain de vérifier l'approbation de l'ordre. Au contraire, un tel ordre frauduleux est nul justement parce que l'expression de volonté du prétendu donneur d'ordre ne pouvait pas avoir lieu.

L'authentification de l'ordre de paiement est indispensable sur Internet où l'ordre pourrait s'exposer à la fraude plus fréquemment qu'en réseau fermé. En plus, contrairement au monde matériel, l'espace dématérialisé est propice aux altérations sans traces.

26 Deuxièmement, l'efficacité de l'ordre de paiement peut souffrir de la révocabilité de l'ordre. L'ordre de paiement s'analyse comme un mandat. Le mandat est traditionnellement révocable. D'après l'article 2004 du Code civil français « le mandant peut révoquer sa procuration quand bon lui semble […] ». Il est clair que l'irrévocabilité de l'ordre de paiement par l'ayant droit dont il émane est indispensable pour que l'ordre débouche sur le paiement. C'est pour cela que le législateur consacre quelque fois l'irrévocabilité de l'ordre de paiement. Au niveau communautaire, la recommandation du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique incite également, sous certaines réserves, à l'irrévocabilité des ordres de paiement.

27 Ainsi, s'assurer de l'efficacité de l'ordre de paiement nécessite tout d'abord la vérification d'approbation et l'authentification de l'ordre de paiement sur Internet, ce qui retiendra notre attention au titre 1. Un tel ordre de paiement reste efficace s'il ne peut pas être révoqué. La problématique de l'irrévocabilité de l'ordre de paiement sur Internet fera l'objet du titre 2.

TITRE 1

La vérification d'approbation et l'authentification de l'ordre de paiement sur Internet

28 Il existe un concept juridique qui a la vertu de relier la vérification d'approbation et l'authentification de l'ordre de paiement sur Internet. Il s'agit de la signature électronique. Cette notion a été récemment introduite dans le droit de la preuve. Ainsi, nous commercerons par l'étude du concept de la signature électronique en droit de la preuve (chapitre 1).

Pour connaître jusqu'à quel point l'approbation et l'authentification sont exploitées pour contribuer à l'efficacité de l'ordre de paiement sur Internet, nous analyserons ensuite le degré d'implantation des signatures électroniques dans divers solutions de paiement (chapitre 2).

CHAPITRE 1

Le concept de signature électronique en droit de la preuve

29 Les différentes méthodes d'identification ou d'authentification dans l'espace virtuel se développent depuis la naissance de la communication électronique. Mais ce n'est que durant la dernière décennie que des initiatives d'appréhension, par le droit, de ces méthodes commencent à apparaître. Il s'agit d'attribuer certains effets juridiques à ces méthodes.

En relation avec les actes juridiques, les méthodes d'identification ou d'authentification peuvent juridiquement servir non seulement à prouver l'identité de l'auteur de l'acte, mais aussi à prouver que l'auteur a voulu les conséquences juridiques de l'acte. Traditionnellement, telles sont les fonctions de la signature[28].

30 Les actes juridiques passés sur Internet nécessitaient aussi une signature qui remplirait les mêmes fonctions. Ainsi, de nombreux États et certains organismes internationaux ont entrepris les travaux législatifs qui ont donné naissance au concept de la signature électronique. Dans les droits latins, qui connaissent le régime de la preuve légale limitant l'admissibilité des modes de preuve[29], la reconnaissance de la signature électronique et donc des actes signés électroniquement était un événement encore plus important que dans les autres droits[30].

Il convient premièrement d'exposer certaines définitions de la signature électronique retenues par les textes (section 1). Deuxièmement, nous nous pencherons sur la question de la force probante de l'ordre de paiement signé électroniquement (section 2).

Section 1

Les définitions de la signature électronique

31 Une multitude de définitions de la signature électronique est issue de l'activité législative et réglementaire dans le monde entier. Les premiers efforts de définition aux États-Unis peuvent être datés de 1991 lorsque le Comité de la sécurité des informations de l'Association des barreaux américains a commencé à travailler sur le projet de loi-modèle sur les signatures numériques. Depuis ce temps-là, de nombreux textes incluant les définitions de la signature électronique et/ou numérique ont été adoptés au niveau des États membres et de l'État fédéral (§ 1.). La Commission des Nations Unies pour le droit commercial international (CNUDCI) a, quant à elle, soigneusement élaboré deux textes qui touchent notre sujet (§ 2.). Entre temps, certains États européens ont entrepris les réformes

[28] A. BENSOUSSAN, « Signature électronique et preuve : évolution ou révolution », *RJC* janvier 2001, n° spécial, Le droit des affaires du XXI^e^ siècle, p.43.

[29] En France, les ordres de paiement donnés par les non-commerçants et excédant la somme de 5 000 F ne pouvaient être prouvés, sauf convention contraire, que par les actes sous seing privé ou les actes authentiques.

[30] Les droits germaniques, ainsi que le droit des pays de la Common Law.

de leur droit de la preuve (comme l'Allemagne ou l'Italie)[31]. La France a également suivi cette voie en adoptant la loi n° 2000-230 du 13 mars 2000 qui transpose déjà la directive communautaire du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (§ 3.).

§ 1. Les textes des États-Unis

32 Les États-Unis ont déjà cinq ans d'expérience avec les textes sur les signatures électroniques. Ainsi, il peut être particulièrement intéressant de suivre l'évolution législative américaine.

Les textes relatifs à la signature électronique ou numérique sont aujourd'hui très nombreux aux États-Unis[32]. Souvent, un seul État dispose de plusieurs textes dont les champs d'application diffèrent. D'où l'apparition des définitions de portée inégale. La plupart de temps, ces textes distinguent entre la signature électronique et la signature numérique (A.).

Or, depuis deux ans, les tendances vers l'uniformisation des textes d'origine étatique, qui devraient en plus devenir technologiquement neutres, se font sentir dans les lois fédérale et uniforme (B.).

A. La signature électronique et la signature numérique

33 La première initiative visant l'adaptation du droit aux technologies de l'information est venue de l'Association des barreaux américains qui, préparant dès 1991 une loi-modèle, a finalement délivré son travail sous forme de lignes directrices. C'était en été 1995. Inspirée par ces lignes directrices, l'Utah a adopté la première loi sur les signatures numériques, amendée en 1996[33]. D'autres États l'ont suivi, comme le Minnesota et l'État de Washington.

Cette première vague de textes reconnaît les signatures numériques comme un type de signatures électroniques fondé sur la cryptographie asymétrique et la certification par les tiers certificateurs[34].

34 En 1997, l'Illinois a adopté un texte qui a amorcé une deuxième vague législative. Dans ce modèle, la loi reconnaît les signatures électroniques en général, mais les effets juridiques renforcés sont accordés aux signatures électroniques sécurisées basées sur les technologies soit directement approuvées par la loi, soit certifiées par les organes de l'État. Parmi ces technologies figure la cryptographie asymétrique à tierce certification.

Donc, ni les lois issues de la première vague, ni les lois empruntant leurs formulations au deuxième modèle, ne sont technologiquement neutres. Elles accordent la supériorité juridique à l'infrastructure à clé publique qui est perçue comme un procédé sûr.

---

[31] Ph. NATAF et J. LIGHTBURN, « La loi portant adaptation du droit de la preuve aux technologies de l'information », *JCP* éd. E 2000, p. 836 : T. HASSLER, « La signature électronique ou la nouvelle frontière probatoire », *RJC* 2000, p. 194.

[32] Pour les listes de lois et les définitions, voir http://www.mbc.com/ecommerce/legislative.asp .

[33] H. ABELSON et L. LESSIG, « Digital Identity in Cyberspace », White Paper Submitted for 6.805/ Law of Cyberspace: Social Protocols, 10 December 1998, p. 57.

[34] P. BRUMFIELD FRY, « A PreliminaryAnalysis of Federal and State Electronic Commerce Laws », 2000, www.uetaonline.com/docs/pfry700.html .

Deux textes plus récents, the Uniform Electronic Transaction Act (UETA) et the Electonic Signature in Global and Nation Commerce Act (E-Sign), veulent pallier cette « discrimination » des autres signatures électroniques.

B. L'uniformisation et la neutralité technologique

35 En juillet 1999, pendant sa réunion annuelle, la Conférence nationale des Commissionnaires pour les lois uniformes des Etats (the National Conference of Commossioners on Uniform State Laws) a adopté et recommandé pour adoption par les États la « loi uniforme des transactions électroniques » connue sous le sigle d'UETA. Ce texte représente une loi uniforme qui n'est ni une loi relative aux contrats électroniques, ni une loi sur les signatures numériques. Elle a déjà été adoptée par la plupart des États membres.

L'article 2 (en anglais « section 2 ») d'UETA contient une définition de la signature électronique. Il dispose que « la "signature électronique" est un son électronique, un symbole ou un procédé qui attaché ou logiquement associé à l'écrit et accompli ou accepté par la personne avec l'intention de signer l'écrit »[35]. Cette définition assure simplement que la signature peut être accomplie par les moyens électroniques. Elle emploie même le terme « signer », cela pour marquer que le sens de la signature est déterminé par d'autres lois applicables. Aucune technologie spéciale n'est nécessaire pour créer une signature valide. D'après le commentaire figurant sous l'article, le clic sur une page web suffit pour signer, dès que l'intention de signer est présente. La signature utilisant la cryptographie à clé publique est incluse dans cette définition.

36 Nous retrouvons une définition presque identique à celle d'UETA dans la « loi sur les signatures électroniques dans le commerce global et national » dite E-Sign. Il s'agit d'une loi fédérale signée par le Président des États-Unis le 30 juin 2000. Bien qu'elle n'ait pas pour but d'enrayer les initiatives législatives des États membres dans ce domaine, elle y pose des limites. E-Sign permet l'adoption d'UETA par les États, mais les exceptions qui y étaient possibles sont limitées. Section 102(a)(2)(A) dispose que les modifications ne pourraient pas accorder un effet ou un statut juridique plus important à l'application de certaines technologies aux signatures électroniques.

Or, comme nous l'avons vu plus haut, c'est justement ce que les textes des deux premières vagues des lois sur les signatures électroniques font. E-Sign interdisant de telles mesures, ces textes antérieurs ne peuvent plus être applicables.

37 Nous verrons que l'approche américaine qui, pour satisfaire au postulat de la totale neutralité technique des signatures électroniques, n'accepte pas la fiabilité comme élément de la définition, n'est pas celle de la Commission des Nations Unies pour le droit commercial international (CNUDCI).

[35] UETA avec préface et commentaires est disponible à l'adresse www.uetaonline.com .

§ 2. Les textes de la CNUDCI

38 La CNUDCI a élaboré deux textes qui traitent des signatures électroniques. Il s'agit de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique de 1996 et 1998[36]. La définition de la signature électronique contenue dans la Loi type a été reprise, avec certains remaniements et complètements, dans le projet de la Loi type de la CNUDCI sur les signatures électroniques tel qu'approuvé par le Groupe de travail de la CNUDCI sur le commerce électronique en septembre 2000[37].

Bien que ces textes soient très proches, nous pouvons déceler une divergence dans les définitions (A.). Ensuite, par rapport à la Loi type sur le commerce électronique, le projet de la Loi type sur les signatures électroniques ajoute une présomption de fiabilité de la signature électronique (B.).

A. Une divergence dans les définitions

39 La loi type sur le commerce électronique désigne comme signature électronique, sans employer cette notion, toute méthode qui « est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données » et dont « la fiabilité […] est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière ». Ces méthodes sont mises à pied d'égalité avec les signatures traditionnelles.

40 Le projet de la Loi type sur les signatures électroniques comprend la définition dans son article 2. Par rapport à la Loi type sur le commerce électronique, la notion de signature électronique y apparaît plus large. Elle désigne « des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue ». Or, en vertu de l'article 6, seules les signatures électroniques qui répondent à l'exigence de la fiabilité suffisante équivalent aux signatures manuscrites.

41 Nous pensons que la définition de la Loi type sur le commerce électronique est meilleure. En fait, le projet de la Loi type sur les signatures électroniques forge une définition large de la signature électronique, mais n'accorde pas l'effet juridique d'une signature aux signatures électroniques qui ne satisfont pas à la fiabilité requise. Pourquoi alors appeler « signature » électronique quelque chose qui n'a pas les effets d'une signature ? Le projet de guide pour l'incorporation de la Loi type sur les signatures électroniques n'a pas passé outre ce problème. Il remarque qu'il est nécessaire de distinguer entre la notion juridique de « signature » et la notion technique de signature électronique[38].

Mais l'article 6 du projet de la Loi type sur les signatures électroniques est bienvenu en ce qu'il consacre une présomption de fiabilité de la signature électronique pour certaines méthodes utilisées pour signer.

---

[36] Disponible sur www.uncitral.org/fr-index.htm .

[37] Voir le « Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques » du 17 mai 2001, www.uncitral.org/fr-index.htm .

[38] Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques, document A/CN.9/493, p. 40, n° 94, www.uncitral.org/fr-index.htm .

B. La présomption de fiabilité de la signature électronique

42 Le paragraphe 3 de l'article 6 du projet de la Loi type de la CNUDCI sur les signatures électroniques dispose que dans certains cas, la signature électronique est considérée fiable[39]. C'est parce que les procédés techniques valant signature électronique remplissent dans ces cas les critères objectifs qui permettent de conclure au préalable que la signature sera fiable.

Cette disposition se présente donc comme une présomption de fiabilité, c'est-à-dire que le procédé qui satisfait aux conditions de ce paragraphe est reconnu comme signature électronique avant qu'il ne soit effectivement utilisé. Cela apporte une certitude aux utilisateurs de ces procédés.

Il faut remarquer que cette présomption de fiabilité est conçue comme une présomption simple, car le paragraphe 4 permet d'apporter des preuves de la non-fiabilité de la signature électronique.

En plus, bien que certains procédés techniques se trouvent ainsi avantagés, le projet de la Loi type sur les signatures électroniques respecte encore, de façon moins radicale que les nouveaux textes américains, la neutralité technologique des signatures électroniques. La présomption de fiabilité peut bénéficier même aux procédés qui ne sont pas fondés sur le type spécifique de l'infrastructure à clé publique avec la certification d'un tiers. Et surtout, d'un autre côté, même une signature électronique objectivement non sécurisée peut être reconnue fiable compte tenu des circonstances dans lesquelles elle a été utilisée.

43 Il nous semble que l'article 7 de la Loi type de la CNUDCI sur le commerce électronique et le projet de la Loi type sur les signatures électroniques créent un dispositif clair et équilibré, relativement souple, mais pourtant sécurisant. Il est regrettable que les formulations de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques ne soient pas aussi élégantes, mais nous montrerons dans l'exemple français que cela peut ne pas avoir de conséquences sur la qualité du texte transposant la directive.

§ 3. La directive communautaire et les textes français

44 Les Communautés européennes se sont dotées d'un cadre juridique pour les signatures électroniques le 13 décembre 1999 lorsque le Parlement européen et le Conseil de l'Union européenne ont adoptés la directive 1999/93/CE (A.). La directive devait être transposée dans les droits nationaux avant le 19 juillet 2001. La France a rempli cette obligation en adoptant la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique et son décret d'application n° 2001-272 du 30 mars 2000 (B.).

---

[39] Une signature électronique est considérée fiable […] si:
a) Les moyens utilisés pour la création d'une signature électronique sont, dans le contexte dans lequel ils sont utilisés, liés exclusivement au signataire;
b) Les moyens utilisés pour la création d'une signature électronique sont, au moment de la signature, sous le contrôle exclusif du signataire;
c) Toute modification apportée à la signature électronique après le moment de la signature est décelable; et,
d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à l'information après le moment de la signature est décelable.

A. La directive 1999/93/CE

45 Les définitions des signatures électroniques sont situées dans l'article 2, paragraphes 1 et 2, et sont encore enrichies par l'article 5. Ces articles, dont la qualité de rédaction est visiblement insatisfaisante, contiennent des dispositions qui rappellent quelquefois celles de la Loi type de la CNUDCI sur les signatures électroniques. Or, elles ne sont ni aussi claires, ni technologiquement neutres.

46 Premièrement, la directive distingue entre la signature électronique et la signature électronique avancée, mais elle y ajoute encore une catégorie qui pourrait être nommée « renforcée »[40].

La définition de la signature électronique « simple » n'est pas satisfaisante. Elle s'accommode mal à la notion classique de signature[41], car elle omet une fonction essentielle des signatures, à savoir l'approbation de l'acte signé.

En décortiquant l'article 5 de la directive qui est consacré aux effets juridiques des signatures électroniques, nous découvrons que la définition des signatures électroniques avancées de l'article 2, paragraphe 2, est inutile. Elle sert seulement de base pour la définition des signatures électroniques « renforcées ». Par contre, le texte opère une importante distinction entre les signatures électroniques et les signatures électroniques renforcées. Il insiste sur le fait que les États membres reconnaissent les fonctions d'une signature manuscrite aux signatures électroniques « renforcées ». Les autres signatures électroniques, c'est-à-dire même les signatures électroniques avancées[42], se voient accordées les effets juridiques moindres.

47 Deuxièmement, une autre remarque doit être faite à l'égard de la relation entre les signatures électroniques « renforcées » et les procédés techniques satisfaisant cette définition. Par l'utilisation des notions de certificat qualifié et de dispositif sécurisé de création de signature, notions qui sont très techniquement définies à l'article 2 de la directive, avec les renvois aux annexes, la directive reconnaît comme « renforcées » seules les signatures numériques à base de cryptographie asymétrique avec la tierce certification.

48 Cela veut dire que la directive n'accorde expressément les effets juridiques des signatures qu'aux signatures numériques certifiées. Le texte ne dit pas si et dans quelles conditions il était convenable d'accorder les mêmes effets à d'autres procédés techniques. Dans cette perspective, la loi française du 13 mars 2000 apparaît plus claire.

---

[40] La nouvelle loi allemande, en vigueur depuis le 22 mai 2001, transposant la directive et abrogeant l'ancienne loi de 1997, utilise la notion de « signature électronique qualifiée ». Le texte allemand, ainsi que sa traduction non-officielle en anglais est disponible sur le site de *Cyberbanking & Law*, http://rechtsinformatik.jura.uni-sb.de/cbl/cbl-statutes.php .

[41] D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sou forme électronique », *J.T.* 2001, p. 116. L'article est reproduit sur le site de *Droit et nouvelles technologies*, www.droit-technologie.org/fr/index.asp .

[42] La signature électronique avancée est définie comme « une signature électronique qui satisfait aux exigences suivantes :

a) être liée uniquement au signataire ;

a) permettre d'identifier le signataire ;

a) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif

et

a) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

B. La loi française du 13 mars 2000 et son décret d'application

49 La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique a, entre autre, inséré dans le Code civil un nouvel article 1316-4 relatif aux signatures en général et aux signatures électroniques en particulier (1.). Cet article est complété par le décret n° 2001-272 du 30 mars 2001 (2.).

1. L'article 1316-4 du Code civil

50 La conception de l'article 1316-4 nous paraît comme une combinaison de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique et de la conception du projet de la Loi type de la CNUDCI sur les signatures électroniques.

La loi française a choisi une définition étroite de la signature électronique, comme la Loi type sur le commerce électronique. L'alinéa 1 de l'article 1316-4 Code civil définit tout d'abord la signature en général comme un procédé d'identification et d'approbation. Ensuite, l'alinéa 2 dispose que la signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

A l'instar du projet de la Loi type sur les signatures électroniques, la deuxième phrase de l'alinéa 2 de l'article 1316-4 du Code civil pose une présomption réfragable de fiabilité pour certaines méthodes. Pour les détails, le Code civil renvoie au décret d'application.

51 Comme nous l'avons déjà mentionné, nous estimons la qualité de cet article du Code civil satisfaisante. Un petit problème résulte pourtant de sa concision. Lorsque le texte dispose que la signature électronique consiste en l'usage d'un procédé fiable, il ne précise pas si cette fiabilité doit être évaluée objectivement ou, comme le précise le projet de la Loi type sur les signatures électroniques, compte tenu des circonstances.

2. Le décret n° 2001-272 du 30 mars 2001

52 Le décret d'application est une transposition assez fidèle de certains articles et de toutes les annexes de la directive communautaire sur les signatures électroniques. Son article 2 limite le bénéfice de la présomption de fiabilité à la signature numérique reposant sur l'infrastructure à clé publique avec la certification qualifiée.

Nous ne pouvons qu'exprimer le regret que la présomption de fiabilité ne profite qu'à ce procédé spécifique, ce qui pourrait entraver la recherche d'autres méthodes d'identification et d'approbation plus performantes. Mais cette observation est tempérée par le fait qu'il s'agit de la disposition d'un décret qui est susceptible de modifications plus rapides qu'une loi.

53 Nous avons vu plusieurs variations sur le même thème – la reconnaissance des méthodes électroniques d'identification et d'approbation comme équivalents fonctionnels des signatures manuscrites.

Quelle est la conséquence de cette reconnaissance ? Les actes signés par ces équivalents fonctionnels reçoivent les effets juridiques des actes sous seing privé, c'est-à-dire qu'ils acquièrent une certaine force probante, au moins en droit français.

Nous allons étudier la force probante qu'acquiert un ordre de paiement signé électroniquement pour pouvoir en déduire si les signatures électroniques représentent des mesures soutenant l'efficacité des ordres de paiement.

Section 2

La force probante de l'ordre de paiement signé électroniquement

54 La force probante de l'ordre de paiement signé électroniquement, c'est-à-dire la foi qu'il faut lui attacher[43], est étroitement liée aux fonctions de la signature. Deux fonctions sont inhérentes à la signature dans le monde entier, à savoir l'identification du signataire et l'expression d'approbation de l'acte signé. D'où, nous pouvons déduire que la force probante de l'ordre de paiement signé concernera la preuve de l'identité du donneur d'ordre de paiement (§ 1.) et la preuve de l'approbation de l'ordre de paiement (§ 2.). L'utilisation des procédés techniques spécifiques peut conférer à la signature électronique même la fonction de vérification de l'intégrité de l'acte signé. Ainsi, l'ordre de paiement muni d'une signature numérique permettra de fournir la preuve de l'intégrité de l'ordre de paiement (§ 3.).

§ 1. La preuve de l'identité du donneur d'ordre de paiement

55 L'ordre de paiement qui a été signé à l'aide d'une signature électronique permet, dans certain cas, d'apporter la preuve de l'identité du donneur d'ordre. Ces cas diffèrent d'après la conception de la signature électronique. Il s'agit des situations où soit, la signature électronique n'a pas été désavouée par le prétendu signataire ou il a été retenu après les vérifications que la signature est imputable au signataire, soit, le prétendu signataire n'a pas pu fournir la preuve contraire détruisant la présomption d'imputabilité de sa signature.

Alors, il apparaît qu'aujourd'hui, deux systèmes de preuve d'identité existent, celui de la preuve par vérification d'imputabilité (A.) et celui de la preuve par présomption d'imputabilité (B.). Ils peuvent être combinés au sein d'un seul ordre juridique, comme c'est le cas de la France.

A. La preuve par vérification d'imputabilité

56 La preuve par vérification d'imputabilité est un système classique des droits de la preuve. Il suffit que le prétendu signataire désavoue la signature apposée à l'acte. Cela engendre la vérification de son imputabilité au prétendu signataire. La charge de la preuve revient à celui qui se prévaut de l'acte contre le prétendu signataire.

57 Aux États-Unis, « the Uniform Electronic Transaction Act » sus-mentionné dispose dans son article 9 (section 9) que « l'écrit ou la signature électroniques sont imputables à la personne s'ils étaient le fait de la personne. Le fait de la personne peut être démontré de manière quelconque […] ». Le commentaire sous cet article remarque que la disposition ne change pas les règles d'imputabilité traditionnelles de la signature[44].

---

[43] *Vocabulaire juridique*, sous la direction de G. CORNU, Association Henri Capitant, Quadrige/Presses Universitaires de France, 2000.

[44] UETA avec préface et commentaires, www.uetaonline.com , p. 35.

58 Dans le Code civil français, ce système est instauré par les articles 1323 et 1324. Ces derniers s'appliquent aux actes sous seing privé, donc aussi aux actes sous seing privé électroniques, ce qui inclut les ordres de paiement signés électroniquement.

Mais, la dénégation de la signature électronique sera quelque peu spécifique par rapport à la signature manuscrite. Le Code civil entre dans la catégorie des lois qui n'ont reconnu les fonctions des signatures manuscrites qu'aux procédés techniques fiables. Cette fiabilité devra être vérifiée pour pouvoir conclure que les actes ainsi signés équivalent aux actes sous seing privé. Or, la vérification devrait nécessairement concerner la fiabilité d'identification. Ainsi, le prétendu signataire n'aura plus intérêt à désavouer la signature si le procédé d'identification, grâce aux moyens de preuve apportés par la partie adverse, a été reconnu fiable.

Plus important encore, pour certains actes sous seing privé électroniques, le Code civil a implicitement consacré un autre système, celui de la preuve par présomption d'imputabilité.

B. La preuve par présomption d'imputabilité

59 Comme nous l'avons déjà mentionné plus haut, l'article 1316-4, alinéa 2, deuxième phrase du Code civil français a instauré une présomption de fiabilité pour certains procédés d'identification qui, s'ils garantissent encore le lien entre l'acte et la signature, constituent les signatures électroniques. La fiabilité est présumée, jusqu'à preuve contraire, lorsque, entre autre, « l'identité du signataire [est] assurée […] dans des conditions fixées par le décret en Conseil d'État ».

60 Bien que la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique n'ait pas touché aux articles relatifs à l'acte sous seing privé, elle a implicitement créé un autre régime de dénégation de la signature électronique consistant en l'usage des procédés qui bénéficient de la présomption de la fiabilité.

Si, d'une part, la fiabilité des procédés suppose l'identité du signataire assurée et, de l'autre part, celui qui se prévaut d'une telle signature n'a pas à démontrer la fiabilité des procédés utilisés, nous pouvons conclure que celui qui se prévaut d'une telle signature n'a pas à démontrer que l'identité du signataire est assurée. Cela revient à dire que l'imputabilité au signataire est présumée.

Ainsi, pour dénier l'imputabilité de la signature, le prétendu signataire devra fournir la preuve contraire pour renverser la présomption[45]. La charge de la preuve est ici renversée par rapport à ce que dispose l'article 1324 du Code civil.

61 Certains textes américains, présentés plus haut comme la première et la deuxième vague de la législation sur les signatures numériques et électroniques, comportent aussi la présomption de l'imputabilité, mais cette fois de façon expresse. Car toutes les signatures électroniques ne peuvent pas bénéficier de cette présomption, ces dispositions se trouvent depuis l'entrée en vigueur de ladite E-sign privées d'application comme contraire au postulat de la neutralité technologique de la réglementation.

62 Il résulte de ce qui a été exposé que l'ordre de paiement signé à l'aide d'un procédé qui bénéficie de la présomption de fiabilité aura son imputabilité à la personne désignée

[45] D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sou forme électronique », *J.T.* 2001, p. 119. L'article est reproduit sur le site de *Droit et nouvelles technologies*, www.droit-technologie.org/fr/index.asp .

garantie. Dans les autres cas, où l'imputabilité devra être prouvée, seuls les procédés qui permettent une bonne vérification d'identité pourront figurer comme preuve de l'identité du donneur d'ordre.

§ 2. La preuve de l'approbation de l'ordre de paiement

63 Mis à part quelques textes américains qui, à côté de la présomption d'imputabilité, posent la présomption d'approbation de l'acte si celui-ci a été signé par une sorte spéciale de signature électronique, des réglementations se taisent au sujet de la preuve de l'approbation de l'acte. Il est pourtant possible de déduire les solutions du concept même de la signature.

64 Tant dis que le Code civil français ou les Lois types de la CNUDCI précitées comprennent l'approbation de l'acte comme l'une des fonctions de la signature, l'UETA ou l'E-sign américaine insistent toujours sur le fait que la signature suppose l'intention de signer, c'est-à-dire de faire un acte juridiquement significatif[46].

65 Il nous paraît alors possible de penser que le Code civil français ou les Lois types de la CNUDCI raisonnent dans le sens de la signature vers l'approbation de l'acte, alors que les textes américains le font à l'envers. Suivant le premier raisonnement, l'approbation de l'acte – dans notre cas de l'ordre de paiement – sera sous-entendue dans la notion de la signature, tout comme l'imputabilité à la personne désignée par l'acte. Or, contrairement au régime de l'imputabilité, le Code civil français ne connaît pas la simple dénégation de la signature pour la seule absence de volonté d'approuver l'acte. Ainsi, selon les règles classiques de la charge de la preuve de l'article 1315 du Code civil, celui qui invoque l'absence d'approbation doit la prouver.

Ce problème a été aussi ressenti pendant les travaux sur le projet de la Loi type de la CNUDCI sur les signatures électroniques. Le projet de guide pour l'incorporation de cette Loi type a finalement conclu qu'en « apposant une signature (qu'elle soit manuscrite ou électronique) à une information, le signataire devrait être réputé avoir approuvé l'établissement d'un lien entre son identité et cette information »[47].

En droit américain, la situation paraît être inverse. Celui qui se fonde sur un acte signé doit, tout d'abord, prouver qu'il s'agit de la signature, c'est-à-dire que le signataire a voulu approuver l'acte, car l'approbation est une condition *sine qua non* de la signature.

66 Il nous semble que ces deux concepts de signature quant à l'approbation de l'acte coïncident avec les approches adoptées quant aux exigences sur les procédés qui peuvent valoir signature. Le droit américain est, dans ce dernier aspect, particulièrement libéral ce qu'il doit compenser par le contrôle de l'approbation de l'acte.

---

[46] UETA avec préface et commentaires, www.uetaonline.com , p. 13.

[47] Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques, document A/CN.9/493, p. 48, n° 120, www.uncitral.org/fr-index.htm .

§ 3. La preuve de l'intégrité de l'ordre de paiement

67 La signature manuscrite n'assure pas l'intégrité de l'acte signé. Or, le support papier rend le plus souvent décelable l'altération de l'acte et donc permet la vérification de l'intégrité.

Tel n'est pas le cas du support électronique qui rend possibles les altérations sans traces. Mais, ce problème peut être résolu en utilisant les procédés de la cryptographie asymétrique. La signature numérique étant un cryptage de l'écrit abrégé par la méthode de hachage, il existe une signature unique à chaque écrit. Si le document est frauduleusement altéré, l'abrégé obtenu par le décryptage de la signature originaire ne correspondra pas à l'abrégé du document reçu. L'altération est décelable.

68 Le Code civil dispose, dans son article 1316-4, alinéa 2, deuxième phrase, que la fiabilité du procédé d'identification est présumée, entre autre, lorsque l'intégrité de l'acte est garantie, dans les conditions fixées par le décret d'application. De ce fait, les procédés reconnus comme objectivement fiables par le décret, et donc bénéficiant de la présomption de fiabilité, doivent respecter cette garantie d'intégrité de l'acte. D'où, les ordres de paiement signés par ces procédés recevront la présomption d'intégrité.

69 Nous avons étudié différentes acceptions de la notion de signature électronique et ensuite, nous avons analysé la force probante des ordres de paiement signés électroniquement. Nous pouvons conclure ce chapitre en énonçant que, dans certaines conditions, l'adjonction de la signature électronique peut réellement aider à soutenir l'efficacité de l'ordre de paiement, c'est-à-dire son aboutissement au paiement. C'est parce que certaines conceptions de signature électronique garantissent l'imputabilité de l'ordre de paiement signé électroniquement au donneur d'ordre désigné par l'ordre, elles garantissent l'approbation de l'ordre et, quelque fois, même l'intégrité de l'ordre. Dans ce dernier cas, la signature électronique répond donc à l'exigence de vérification d'approbation et de l'entière authentification.

Les signatures électroniques peuvent alors contribuer à l'efficacité des ordres de paiement. Encore, faut-il que ces ordres soient électroniquement signés. Pour connaître la réelle efficacité des ordres de paiement, nous devrons procéder à la recherche du degré d'implantation de signatures électroniques dans diverses solutions de paiement.

CHAPITRE 2

Le degré d'implantation de la signature électronique dans diverses solutions de paiement

70 Nous avons démontré que les signatures électroniques attachées aux ordres de paiement peuvent juridiquement sécuriser le paiement. Il convient alors de se poser la question si les signatures électroniques sont souvent utilisées en relation avec les ordres de paiement. Pour pouvoir répondre, il faut analyser les différentes solutions de paiement existant sur

Internet[48].

Cette étude aura pour base la réglementation française des signatures électroniques. Nous examinerons d'abord les solutions aux ordres de paiement sans signatures électroniques (section 1). Après, les solutions aux ordres de paiement signés électroniquement seront présentées (section 2).

Section 1

Les solutions aux ordres de paiement sans signatures électroniques

71 Si nous revenons encore une fois à la définition de la signature électronique de l'article 1316-4 du Code civil, nous observons qu'elle pose deux exigences, d'une part, l'usage d'un procédé fiable d'identification et, de l'autre part, le lien de cette signature potentielle à l'acte auquel elle s'attache. Il existe alors deux situations où les ordres de paiement ne sont pas signés électroniquement. Premièrement, il s'agit des solutions de paiement sans procédés fiables d'identification (§ 1.). Deuxièmement, il existe des solutions avec des procédés fiables d'identification (§ 2.) mais qui n'ont pas de lien avec l'ordre de paiement.

§ 1. Les solutions sans procédés fiables d'identification

72 Les solutions de paiement sans procédés fiables d'identification sont celles qui ne vérifient aucunement l'imputabilité de l'ordre de paiement à la personne dont les données bancaires, comme le numéro apparent de la carte de paiement et sa date d'échéance, figurent dans l'ordre. Peu importe si ces données à caractère personnel transitent par Internet sous forme cryptée ou non.

73 L'envoi du numéro apparent de la carte de paiement est la technique quantitativement la plus répandue d'ordre de paiement sur Internet[49]. Une telle utilisation de la carte de paiement est permise par l'article 6-5 du contrat « Carte bancaire » qui autorise l'émetteur de la carte à débiter le compte du titulaire de la carte sur le vu des enregistrements ou relevés transmis par le commerçant, même en l'absence de factures signées par le titulaire ou assorties d'un contrôle du code confidentiel[50].

Le numéro à 16 chiffres d'identification de la carte de paiement, s'il n'est pas crypté,

[48] Pour une database très complète et régulièrement mise à jour, voir « *e*PSO Inventory Database » sur http://epso.jrc.es .

[49] Communication de la Commission européenne « Commerce électronique et services financiers », COM (2001) 66 final du 7 février 2001, p. 17, disponible sur http://europa.eu.int/comm/internal_market/fr/finances/general/ecomfaq.htm ; voir aussi J.-P. BUYLE, « Le paiement sur internet », *J.T.* 2001, p. 130. L'article est reproduit sur le site de *Droit et nouvelles technologies*, www.droit-technologie.org/fr/index.asp .

[50] Lamy Droit du financement, *Cartes de paiement et de crédit*, n° 2410, Éditions Lamy 2001.

peut être intercepté sur le réseau. Il peut être capturé même sur les facturettes et, après, utilisé par un fraudeur sur Internet.

74 Le protocole SSL qui chiffre les données transportées par Internet, ne permet pas non plus la vérification d'imputabilité à la personne désignée par l'ordre de paiement comme son auteur. Il emploie le chiffrement asymétrique, mais pas pour la vérification de l'identité des acteurs. Il ne sécurise que le transfert des données par le réseau.

75 Malgré le haut risque de fraude, ces solutions de paiement sont acceptées par les consommateurs, les commerçants et les établissements de crédit.

Du point de vue du commerçant, la situation est vraiment dangereuse, parce que les articles 3.8 et 3.9 du contrat « Adhésion au système de paiement à distance par carte bancaire CB » laissent le commerçant supporter entièrement les risques du système. La banque est autorisée par ces dispositions à débiter d'office son compte du montant de toute opération de paiement dont la réalité même ou le montant serait contesté par écrit par le titulaire de la carte et le commerçant doit assumer l'entière responsabilité[51] des conséquences dommageables de tout débit contesté par un client[52].

76 Les solutions de paiement sans procédés fiables d'identification existent sous diverses variantes, des plus simples, comme l'envoi du numéro de la carte de paiement au commerçant pour la réservation d'hôtel, aux plus élaborées où l'ordre de paiement est détaché de la commande et le serveur gestionnaire demande l'autorisation auprès de la banque du porteur de la carte, comme c'est le cas de Payline SSL française[53].

§ 2. Les solutions avec procédés fiables d'identification

77 Bien que moins répandues que le simple envoi du numéro de la carte de paiement, les solutions avec les procédés fiables d'identification se développent de plus en plus. Aujourd'hui, l'usage des cartes de paiement, des numéros sécurisés ou des comptes virtuels, combinés avec les codes confidentiels, sont en plein essor. Toutes ces solutions utilisent les procédés fiables d'identification, mais sans l'exploitation de la cryptographie asymétrique le lien des procédés d'identification avec l'ordre de paiement manque.

78 En fait, le lien entre le procédé d'identification et l'ordre de paiement présente un problème technique. Dans le monde réel, la connexité entre l'ordre de paiement sur le support papier et la signature qui y est apposée est naturellement assurée. Par contre, dans l'espace virtuel, il n'est pas aisé de relier le procédé d'identification à un ordre de paiement précis. Le procédé d'identification doit comporter la trace de cet ordre individuel. Pour pouvoir contenir les traces, le procédé d'identification ne devrait pas fonctionner comme un permis d'accès, comme c'est justement le cas des codes confidentiels, mais il devait s'apparenter à un document changeant et unique pour chaque ordre de paiement. C'est pour cela que nous préférerions la notion de « données sous forme électronique » à celle de « procédé d'identification ». D'ailleurs, le projet de la Loi type de la CNUDCI sur les signatures électroniques ainsi que la directive communautaire emploient le terme « données sous forme électronique ».

---

[51] Remarquons que le contrat utilise à tort la notion de responsabilité au lieu du risque.
[52] D. FELIX, « Paiement en ligne, un risque pour les sites marchands », *Les Echos*, 8et 9 déc. 2000, p. 55.
[53] www.payline.com .

79 Ces solutions de paiement ne sont alors juridiquement sécurisées mais elles possèdent un haut degré de sécurité technique. Les solutions basées sur les numéros sécurisés, comme O-card d'Orbiscom[54], Boing de la Bank of Ireland[55], SPA (Secure Payment Application) de Mastercard[56] et bientôt CVD (Carte virtuelle dynamique) en France[57], exploitent le système classique de paiement par carte bancaire. Elles remplacent l'envoi du numéro facial de la carte de paiement par l'envoi d'un numéro spécialement émis par le logiciel pour une transaction après la vérification de l'identité du titulaire de la carte.

80 Une autre solution originale, nommée SafeDebit[58], se développe aux États-Unis. Les données bancaires, d'habitude contenues par exemple dans la puce de la carte bancaire, sont inscrites cryptées sur un CD-ROM qui sert après comme une carte avec le code confidentiel. Les bénéfices de cette solution tiennent dans le fait que le donneur d'ordre de paiement n'a pas besoin d'un lecteur spécial et pourtant le contrôle physique de la carte et la vérification du code confidentiel sont possibles.

81 Enfin, pour les micro-paiements, les comptes virtuels prépayés dont l'usage est assuré par un code confidentiel connaissent un grand essor. Nous pensons ici à Paysafecard[59], solution autrichienne garantissant l'anonymat des consommateurs, ou à Odysseo[60], le « portefeuille virtuel » de BLUE LINE International, surtout utilisé en France. En ce qui concerne ce dernier, il s'agit d'une solution de paiement qui combine le compte virtuel prépayé avec la possibilité de payer par carte bancaire répertoriée chez l'intermédiaire.

82 Toutes les solutions de paiement sus-mentionnées sont dépourvues de la présence de la signature électronique. Mais cela ne veut pas dire qu'une introduction de la signature électronique n'est pas envisageable. Nous pouvons trouver les solutions de paiement analogues qui mettent en œuvre les ordres de paiement signés électroniquement.

Section 2

Les solutions aux ordres de paiement signés électroniquement

83 Parmi les solutions aux ordres de paiement signés électroniquement, nous pouvons distinguer entre les cas d'utilisation de la signature électronique sans présomption de fiabilité (§ 1.) et les cas d'utilisation de la signature avec la présomption de fiabilité (§ 2.).

Nous devons remarquer au préalable qu'aujourd'hui, il n'existe pas encore en France de signature électronique qui pourrait bénéficier de la présomption de fiabilité établie par le Code civil. En fait, le décret d'application du 30 mars 2001 renvoie à plusieurs reprises à un arrêté du Premier ministre et à un arrêté du ministre chargé de l'industrie. Ces textes

---

[54] www.orbiscom.com .
[55] www.bankofireland.ie/html/gws/personal/credit_card/boing/index.html .
[56] www.mastercardintl.com/spa/demo/main/html .
[57] *Actualité bancaire*, n° 449, du 3 mars 2001, p. 3, disponible sur www.afb.fr/ab.htm .
[58] www.safedebit.com .
[59] P. P. SINT, « E-money Solution from Austria: Paysafecard.com », *ePSO Newsletter*, n° 6, mars 2001, disponible sur www.epso.jrc.es .
[60] www.odysseo.com , voir aussi P. BORIES, « Juin 2001, l'Odysseo de Blueline », *JDNet Solutions*, 5 juin 2001, http://solutions.journaldunet.com/0106/010605_blueline.shtml .

importants pour la mise en œuvre des signatures électroniques n'ont pas encore été adoptés.

§ 1. L'utilisation de la signature électronique sans présomption de fiabilité

84 Aujourd'hui, le seul procédé qui peut satisfaire à la définition de la signature électronique du Code civil est l'emploi la signature numérique[61], c'est-à-dire un procédé d'identification basé sur la cryptographie asymétrique. La signature numérique est le seul procédé d'identification qui garantit son lien avec l'acte signé.

Ce procédé consiste dans l'utilisation de deux clés cryptographiques, l'une privée pour chiffrer le message, et l'autre publique, pour le déchiffrer. Elles utilisent des algorithmes qui ne peuvent pas être déduits l'un de l'autre mais qui forment pourtant une paire fonctionnelle. L'ordre de paiement chiffré à l'aide de la clé privé ne peut être déchiffré qu'à l'aide de la clé publique correspondante[62].

85 Pour que l'ordre de paiement puisse être authentifié à travers la signature numérique, il faut trouver un mécanisme supplémentaire, appelé infrastructure à clé publique (ICP), en anglais Public Key Infrastructure (PKI), qui permettrait d'associer une personne particulière à une paire de clés et vérifier ainsi la signature[63]. Le lien entre la clé privée et, dans notre cas, le donneur d'ordre peut être assuré de diverses façons. Or, la seule façon reconnue digne, par l'article 2 du décret d'application de l'article 1316-4 du Code civil, des signatures électroniques bénéficiant de la présomption de fiabilité est l'utilisation d'un certificat électronique qualifié. Le décret ne reconnaît qu'un type spécifique de l'infrastructure à clé publique (ICP).

Cette disposition a des conséquences importantes. Les ordres de paiement signés par une signature numérique dont la vérification n'est pas assurée par un certificat, ne peuvent pas acquérir automatiquement la force probante de l'acte sous seing privé et il faudra au préalable démontrer qu'il sont signés par un procédé fiable d'identification. Pourtant ces potentielles signatures numériques peuvent être très fiables, notamment quand le lien entre une paire de clés et le donneur d'ordre de paiement est assuré par le destinataire de l'ordre lui-même.

86 L'absence d'utilisation des certificats n'est pas le seul cas où la fiabilité du procédé d'identification doit être démontrée. Plus nombreux seront les procédés basés sur les certificats électroniques, mais négligeant l'exigence des certificats électroniques qualifiés. Cette exigence se montre d'avantage problématique. Le certificat électronique qualifié doit être délivré par un prestataire de services de certification électronique qui répond aux exigences du décret d'application. La présomption de conformité à ces exigences n'est prévue que pour les prestataires reconnus comme qualifiés. Or, cette qualification officielle n'est pas obligatoire. Les certificats électroniques prétendus qualifiés peuvent alors voir le jour. La personne qui veut se prévaloir de l'ordre de paiement signé électroniquement doit dans cette situation supporter la charge de la preuve du fait que le prestataire répond aux exigences du décret. Ainsi, pour les signatures numériques basées sur les certificats

[61] E. A. CAPRIOLI, « La loi du 13 mars 2000 », *RDBF* mai/juin 2000, Actualités, n° 106, p. 166.
[62] Les clés peuvent être utilisées aussi à l'envers. Dans ce cas-là, elles remplissent la fonction de confidentialité du message. Ce thème sera aborder dans la seconde partie.
[63] Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques, document A/CN.9/493, p. 24, n° 45, www.uncitral.org/fr-index.htm .

électroniques délivrés par les prestataires de services de certification sans qualification officielle, la présomption de fiabilité de la signature perd tout son sens, car la personne s'en prévalant devra de toute façon apporter la preuve des qualités du prestataire.

87 Il y a une troisième raison, déjà esquissée plus haut, pour laquelle toutes les solutions de paiement aux ordres de paiement signés numériquement rentrent dans la catégorie des solutions utilisant les signatures électroniques sans présomption de fiabilité. Le décret n'accorde cette présomption qu'aux signatures établies « grâce à un dispositif sécurisé de création de signature électronique », c'est-à-dire un logiciel mettant en application la clé cryptographique qui doit être certifié conforme à certaines exigences. Les règles d'évaluation ont été laissées à un arrêté du Premier ministre et donc ne sont pas encore connues.

88 Mais il est maintenant déjà possible de prévoir quelles seront les solutions de paiement utilisant la signature électronique avec présomption de fiabilité. C'est pour cela que nous allons les citer ci-après.

§ 2. L'utilisation de la signature électronique avec présomption de fiabilité

89 Après l'adoption des arrêtés prévus par le décret du 30 mars 2001, le procédé d'identification à cryptographie asymétrique qui utilisera le logiciel certifié conforme, sera basé sur les certificats électroniques portant les mentions exigées par le décret et délivré par les prestataires officiellement qualifiés, sera présumé fiable. Jusqu'à preuve contraire, il vaudra signature électronique.

90 Les solutions de paiement qui incluront très probablement la signature avec présomption de fiabilité seront celles qui reposent sur le protocole SET (Secure Electronic Transaction). Il s'agit d'un protocole de communication spécialement conçu pour le paiement au moyen d'une carte de paiement sur Internet. Le protocole SET avait pour but de devenir un standard technique de sécurisation des transactions par carte sur Internet. Or, jusqu'à aujourd'hui, il n'a pas connu de véritable succès.

En 1998, il n'y avait que 150 banques liées à VISA et 78 liées à Mastercard qui prévoyaient de mettre en œuvre le protocole SET. Il n'y avait que 150 sites commerciaux qui l'acceptaient[64]. Depuis ce temps-là, la situation n'a pas beaucoup changée. Surtout, les États-Unis se sont montrés hostiles à adoption de ce protocole. Il paraît que l'échec de SET est dû plutôt au manque de modèles commerciaux convaincants[65].

91 Le protocole SET met en œuvre, entre autre, la cryptographie asymétrique qui est utilisée pour authentifier tous les acteurs du processus de paiement. Le lien entre les clés cryptographiques et les acteurs du processus est assuré par les certificats. Ces certificats sont délivrés sur trois niveaux.

SETCo, l'autorité de certification du premier niveau, délivre les certificats électroniques aux sociétés de cartes de paiement qui, elles-même, délivrent ensuite les

[64] Rapport d'information de M. Jean-Pierre BRARD du 11 juillet 2001, n° 3229, disponible sur www.assemblee-nationale.fr .

[65] Voir l'nterview « Electronic Payments Technologies are Available but Business Models are Missing (Part 2 of an Interview with Michael Waidner) », *ePSO Newsletter*, n° 4, janvier 2001, disponible sur www.epso.jrc.es .

certificats à leurs banques affiliées. Les banques, à leur tour, délivrent les certificats aux titulaires des cartes et aux commerçants.

92 Plusieurs solutions de paiement appliquant le protocole SET ont vu le jour. Les premières solutions qui sont apparues nécessitaient le téléchargement d'un logiciel spécifique par l'utilisateur. C'était le cas de CyberCash, I-Pay[66] néerlandais et TelePay italien.

En France, le protocole SET a été adapté à l'emploi des cartes à puce. Ainsi, la solution de paiement Cyber-COMM est née. La carte à puce est introduite dans un lecteur sécurisé relié à l'ordinateur. Puis, le titulaire de la carte doit composer son code confidentiel. L'identification réalisée, l'ordre de paiement est chiffré, signé par le logiciel du lecteur et transmis à une passerelle de paiement[67]. Nous pouvons trouver une solution de paiement semblable en Belgique, connue sous le nom de Banxafe[68].

Pour simplifier l'utilisation des solutions mettant en œuvre le protocole SET, les sociétés de cartes de paiement entreprennent des actions pour promouvoir l'utilisation de 3D-SET, variante du protocole SET. Celle-ci remplace le logiciel téléchargé par le client par le logiciel du serveur central auquel le client a accès. La société VISA a annoncé qu'elle envisage de rendre toutes ses banques compatibles avec 3D-SET en octobre 2001.

93 Il faut encore ajouter que le protocole SET qui permet de signer les ordres de paiement donnés au moyen d'une carte reste plutôt un standard de paiement hautement sécurisé pour les professionnels.

94 Nous avons vu que la signature électronique peut authentifier et approuver l'ordre de paiement sur Internet et concourir ainsi à l'efficacité de l'ordre de paiement. Or, nous pouvons conclure que l'implantation de la signature électronique dans les solutions de paiement sur Internet n'atteint qu'un faible degré.

Si l'authentification de l'ordre de paiement ne présente pas de problème majeur pour les solutions de paiement appartenant à la nouvelle vague des systèmes de paiement sur Internet, la preuve de l'approbation de l'ordre de paiement est délicate. Cette situation peut s'avérer dangereuse si l'ordre de paiement tombe sous le régime de la preuve légale, qui couvre par exemple certains actes juridiques en droit civil français. Une convention de preuve, permise par le caractère subsidiaire de l'article 1341 du Code civil, doit être vivement recommandée.

Pour que l'ordre de paiement sur Internet soit pleinement efficace, il faut non seulement disposer de possibilités de vérifier la validité de l'ordre, mais aussi qu'une certaine irrévocabilité de l'ordre de paiement soit assurée.

[66] www.i-pay.com/uk/merchant/index.htm .
[67] Rapport d'information de M. Jean-Pierre BRARD du 11 juillet 2001 précité.
[68] www.banxafe.com .

TITRE 2

L'irrévocabilité de l'ordre de paiement sur Internet : dilemme

95 L'irrévocabilité de l'ordre de paiement est souvent discutée, pourtant rarement sans confusions. Il nous paraît alors nécessaire de préciser le contenu de la notion d'irrévocabilité.

D'après le Vocabulaire juridique de G. CORNU[69], l'irrévocabilité signifie le « caractère de ce qui n'est pas susceptible de révocation unilatérale […] ». La « révocation » d'un acte veut dire un « acte unilatéral de rétractation par lequel une personne entend mettre à néant un acte antérieur dont elle est l'unique auteur […] ». La « rétractation » est comprise comme la « manifestation de volonté contraire par laquelle l'auteur d'un acte ou d'une manifestation unilatérale de volonté entend revenir sur sa volonté et la retirer comme si elle était non avenue, afin de la priver de tout effet passé ou à venir ».

Si nous résumons toutes ces définitions, il en ressort assez clairement que le dilemme révocabilité/irrévocabilité ne concerne que les ordres de paiement réguliers. Ainsi, il faut strictement différencier entre les questions concernant l'irrévocabilité de l'ordre de paiement et les oppositions et autres contestations des ordres frauduleux par la personne autorisée à disposer des fonds sur le compte.

96 Cette courte clarification faite, nous pouvons nous concentrer sur le dilemme de l'irrévocabilité de l'ordre de paiement sur Internet.

Du point de vue du commerçant acceptant le paiement déclenché par l'ordre de paiement sur Internet, l'irrévocabilité de l'ordre de paiement est essentielle. Si l'ordre pouvait être révoqué à l'instant où la livraison du bien a eu déjà lieu, le commerçant s'exposerait à la perte du bien. Il préférerait être payé en espèces. Ou bien il devrait attendre si son compte est crédité ou non. Dans cette situation, il paraît raisonnable d'instaurer le système de l'irrévocabilité absolue.

Or, du point de vue du donneur d'ordre, il y a des situations où l'irrévocabilité de l'ordre de paiement engendre des conséquences trop dures, surtout s'il s'agit du consommateur. Ces situations sont malfaisantes pour le développement du commerce électronique. L'exemple de l'approche des États-Unis montre qu'une certaine révocabilité soutient la confiance des consommateurs dans le paiement sur Internet.

97 En France, il n'existe pas de solution unique au problème de l'irrévocabilité. Ainsi, dans le chapitre 1, nous présenterons la disparité des issues françaises. Le chapitre 2 sera consacré à l'approche cohérente à perspective pro-consumériste telle qu'elle se forme actuellement dans l'Union européenne.

[69] *Vocabulaire juridique*, sous la direction de G. CORNU, Association Henri Capitant, Quadrige/Presses Universitaires de France, 2000.

CHAPITRE 1

La disparité des issues françaises

98 En France, l'ordre de paiement est qualifié par la majorité de la doctrine comme un mandat. Si nous acceptons cette qualification, nous devons constater que le mandat est par principe révocable. Lorsqu'il faut parvenir à son irrévocabilité, celle-ci doit être soit expressément stipulée dans un contrat, soit prévue par la loi.

En analysant les textes, les contrats-cadres, la doctrine et la jurisprudence, nous constatons que les solutions retenues varient selon les moyens de paiement utilisés. La distinction doit être faite entre l'ordre de paiement donné au moyen d'une carte de paiement (section 1) et l'ordre de paiement donné par d'autres moyens de paiement (section 2).

Section 1

L'ordre de paiement donné au moyen d'une carte de paiement

99 Les contrats relatifs à l'usage de la carte de paiement et, plus tard, la loi ont introduit l'irrévocabilité des ordres de paiement donnés au moyen de la carte (§ 1). Tant dis que la doctrine se montrait et se montre encore aujourd'hui parfois réticente (§ 2), la jurisprudence tend à imposer l'irrévocabilité consacrée par le législateur (§ 3).

§ 1. L'introduction de l'irrévocabilité par les contrats et la loi

100 Les émetteurs des cartes de paiement comprenaient l'importance de l'irrévocabilité des ordres de paiement donnés au moyen de la carte pour le système de paiement par carte. Pour cette raison, les contrats passés avec les titulaires des cartes stipulaient que l'établissement émetteur restait étranger à tout différend pouvant survenir entre le titulaire et le fournisseur et que l'existence d'un tel différend ne peut en aucun cas justifier le refus du titulaire de la carte ou du compte d'honorer les règlements par carte. Cette inopposabilité des exceptions tirées de la relation entre le titulaire de la carte et le commerçant impliquait d'après la jurisprudence[70] l'irrévocabilité de l'ordre de paiement. Longtemps, le problème restait réglé uniquement par voie contractuelle[71].

101 Mais, il a semblé plus sûr de prévoir l'irrévocabilité par la loi. L'ordre de paiement donné au moyen de la carte a été déclaré irrévocable par la loi n° 85-695 du 11 juillet 1985. La disposition a été reprise dans l'article 57-2 du décret-loi du 30 octobre 1935 d'où elle est passée à l'article L. 132-2 du Code monétaire et financier.

[70] CA Aix-en-Provence, 18 juin 1984, *D.* 1986, IR., p. 326, note Vasseur.
[71] J. HUET, « Aspects juridiques du télépaiement », *JCP éd. G* 1991, I, 3524, p. 288.

Nous observons pourtant que le contrat « Carte bancaire CB » contient toujours, à l'article 6.7, la clause d'inopposabilité des exceptions et l'article 9 relatif à la recevabilité des oppositions renferme la clause déclarant l'ordre de paiement irrévocable[72]. Vu les positions doctrinales quelquefois réticentes, le maintien de cette clause peut être utile.

§ 2. La doctrine parfois réticente

102 Le texte de la loi a suscité quelques critiques de la part de certains auteurs de la doctrine. D. MARTIN[73], sans démentir l'opportunité de la disposition, considère le mandat et l'irrévocabilité comme deux notions incompatibles, car le mandat est par essence précaire. Ce constat lui sert base pour l'analyse de l'ordre de paiement comme un acte translatif de droit. Donc, il ne nie finalement pas l'irrévocabilité de l'ordre de paiement. Pourtant, l'incompatibilité soutenue entre le mandat et l'irrévocabilité pourrait être dangereuse dans la situation où la plupart de la doctrine voit dans l'ordre de paiement un mandat.

103 Une autre critique concerne plus particulièrement l'ordre de paiement sur Internet. Dans un article récent[74], C. LUCAS de LEYSSAC et X. LACAZE s'interrogent sur la formulation « au moyen d'une carte » contenue dans ladite disposition, plus précisément sur le point de savoir si la seule communication du numéro facial de la carte suffit à caractériser l'ordre de paiement donné au moyen d'une carte. Ils concluent que l'acceptation de la simple communication du numéro d'identification de la carte comme l'utilisation conforme de la carte mènerait à la négation du rôle de la piste magnétique, la puce électronique ou la signature. Ils constatent alors que l'ordre de paiement donné par communication du numéro facial n'est pas irrévocable car il ne peut pas être considéré comme donné « au moyen d'une carte ».

104 Nous ne partageons pas cette opinion doctrinale. Non seulement elle aurait des conséquences graves sur le système de paiement par carte sur Internet mais surtout, elle est bâtie sur les considérations qui ne nous paraissent pas capables de justifier les conclusions.

La fiabilité du moyen de paiement, dans notre cas de la communication du numéro d'identification de la carte de paiement, et l'irrévocabilité de l'ordre de paiement ne sont pas des notions corrélatives. La fiabilité du moyen de paiement ne peut pas avoir d'influence sur la révocabilité ou irrévocabilité de l'ordre. La fiabilité du moyen de paiement est une catégorie qui nous enseigne sur le taux d'ordres frauduleux possibles avec un moyen de paiement précis tant dis que l'irrévocabilité concerne seuls les ordres de paiement émanant d'un ayant droit, c'est-à-dire libres de toute fraude. La fiabilité du moyen de paiement devrait plutôt influencer le partage des risques du système de paiement parmi ses acteurs[75].

Ainsi, nous considérons irrévocables tous les ordres de paiement donnés par n'importe quel usage de la carte, à savoir par la communication du numéro facial de la carte ou du numéro sécurisé périssable, par le contrôle physique de la carte et, en cas de portefeuille

[72] Ce « mariage » spatial des dispositions sur l'irrévocabilité et les oppositions qui a d'ailleurs l'origine dans la loi, explique les nombreuses confusions entre ces institutions différentes.
[73] D. MARTIN, « Analyse juridique du règlement par carte de payement », *D.* 1987, Chron., p. 52.
[74] C. LUCAS de LEYSSAC et X. LACAZE, « Le paiement en ligne », *Communication – Commerce Électronique*, fév. 2001, Chron., p. 15.
[75] Ce problème sera abordé au titre 2 de la seconde partie de cette étude.

virtuel répertoriant les cartes, même par la communication d'un autre élément identifiant la carte dans le répertoire.

105 Contrairement à la doctrine, la jurisprudence s'avère imposer l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte de paiement.

§ 3. La jurisprudence imposant l'irrévocabilité

106 La jurisprudence française admet depuis longtemps l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte[76]. Dans un arrêt du 12 mai 1995, la Cour d'appel de Paris rappelle cette règle en prononçant que « l'apposition de la signature du titulaire de la carte sur l'ordre de paiement confère à celui-ci un caractère irrévocable et abstrait ; le donneur d'ordre doit rembourser les factures réglées par l'émetteur […], sans pouvoir lui opposer aucune exception tirée du rapport fondamental qui a donné lieu au paiement […] »[77].

Même si l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte était admise pour l'ordre passé par la signature de la « facturette », il a fallu attendre encore quelques années jusqu'à ce que la jurisprudence se prononce sur l'irrévocabilité de l'ordre donné par simple communication du numéro de la carte de paiement.

107 Le 8 juin 1999, la Cour d'appel de Paris a rendu un arrêt intéressant notre sujet, bien qu'il s'agisse de l'ordre de paiement passé par fax[78]. L'importance de cet arrêt tient non seulement dans le fait qu'il accepte l'irrévocabilité de l'ordre de paiement donné par simple communication du numéro facial de la carte. Il paraît aussi être le premier à consacrer la validité d'un tel ordre[79] qui est une condition logique de son irrévocabilité.

108 Suite à une conversation téléphonique, Mlle Marcilhacy a envoyé un fax à la société anglaise Byte Indirect en vue de l'achat d'un ordinateur. Le fax contenait son numéro apparent de la carte bancaire de la SA Crédit industriel et commercial (CIC). N'ayant pas obtenu confirmation de sa commande, Mlle Marcilhacy l'a annulée par téléphone. (Elle n'arrive pas à prouver ce dernier événement.) Mais son compte bancaire a été pourtant débité. Elle protestait auprès du CIC qui a recrédité le compte et a établi un bordereau de réclamation. Or, comme la réclamation ne pouvait pas être traitée sans justificatif de l'annulation de la part de Mlle Marcilhacy, son compte a été redébité. Mlle Marcilhacy a alors assigné le CIC en paiement de la somme débitée et en dommages-intérêts. Le tribunal d'instance l'a débouté et elle a interjeté appel.

La cour d'appel de Paris déboute l'appelante et confirme le jugement déféré. Avant de pouvoir faire cette conclusion, la Cour procède à une application parfaitement correcte des dispositions applicables. Elle cite tout d'abord l'article 9 des conditions de fonctionnement de la carte bancaire et l'article 57-2 du décret-loi du 30 octobre 1935 qui, tous les deux, posent la règle de l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte. Après, elle vérifie s'il s'agit d'un ordre de paiement. Ainsi, elle s'assure si Mlle Marcilhacy a passé la commande et si elle a accepté de procéder au règlement de celle-ci au moyen de sa carte bancaire. Donc, la Cour vérifie l'imputabilité de l'ordre à son

[76] CA Aix-en-Provence, 18 juin 1984, *D*. 1986, IR., p. 326, obs. M. Vasseur.
[77] CA Paris, 12 mai 1995, *Rev. dr. bancaire*, nov/déc. 1995, n° 52, p. 217, obs. Crédot et Gérard.
[78] CA Paris, 8e ch. A, 8 juin 1999, Mlle Marcilhacy c/ CIC, *D.* 2000, Somm., p. 337, obs. B. Thullier ; *Dalloz Affaires* 1999, p. 1287, obs. X. D. ; *RTD com*. 1999, p. 939, obs. M. Cabrillac.
[79] Arrêt précité, obs. X. D.

prétendu auteur et l'approbation de l'ordre de paiement, deux conditions sans lesquelles il ne peut pas s'agir de l'ordre de paiement valide. La vérification faite, la Cour d'appel de Paris conclue à l'irrévocabilité de l'ordre de paiement. Quel bel exemple du syllogisme juridique !

109 L'arrêt précité traite le problème de l'ordre de paiement donné par fax. Mais nous considérons ces conclusions transposables à l'ordre de paiement donné au moyen d'une carte sur Internet.

Si l'irrévocabilité de l'ordre de paiement au moyen d'une carte peut alors être acceptée aujourd'hui, les ordres de paiement donnés par d'autres moyens de paiement ne paraissent pas obéir à la même règle.

Section 2

L'ordre de paiement donné par d'autres moyens de paiement

110 L'ordre de paiement donné par d'autres moyens de paiement qu'une carte n'est pas soumis à une réglementation spéciale. Comme les systèmes de paiement sur Internet, mettant en œuvre ces moyens, sont bâtis sur les comptes, bancaires ou non, les ordres de paiement dans de tels systèmes suivront le régime de l'ordre de virement (§ 1). Mais certains aménagements contractuels pourraient créent un autre régime (§ 2).

§ 1. Le régime de l'ordre de virement

111 Outre le système de paiement sur Internet par carte, il existe deux autres systèmes employant les ordres de paiement : le système de virement bancaire à distance par Internet et le système des comptes virtuels. Le premier s'appuie sur les comptes bancaires, tant dis que l'autre sur les comptes gérés par les prestataires de paiement sur Internet. L'ordre de paiement qui mouvemente les fonds est dans les deux cas assimilable à l'ordre de virement traditionnel.

112 L'ordre de virement est un mandat « ordinaire », donc révocable *ad nutum*. La révocabilité disparaît avec son exécution. Le moment précis de l'exécution de l'ordre peut poser des problèmes si l'ordre de virement n'est pas exécuté immédiatement.

D'après la jurisprudence de la Cour de cassation[80], l'ordre de virement présente un caractère révocable jusqu'au moment où le bénéficiaire a acquis un droit sur les fonds par l'inscription du montant du transfert de fonds au débit du compte du donneur d'ordre[81].

Si les ordres de virement à distance par Internet et les ordres de paiement dans le système des comptes virtuels sont exécutés immédiatement, la période de révocabilité de tels ordres, de fait, disparaît.

---

[80] Cass. com., 26 janvier 1983, *D.* 1983, IR 469, obs. M. Vasseur ; *RTD com.* 1984, p. 129, obs. M Cabrillac et B. Teyssié.

[81] T. BONNEAU, *Droit bancaire*, Montchrestien 2001, n° 437.

§ 2. Les aménagements contractuels

113 La révocabilité du mandat n'étant pas d'ordre public, les contrats-cadres instaurant le système de paiement pourraient prévoir l'irrévocabilité de l'ordre de paiement. L'autre possibilité de rendre l'ordre de paiement irrévocable est la stipulation de son exécution immédiate, déjà mentionnée.

114 Nous n'avons pas trouvé de telles dispositions dans ces contrats. Les contrats de systèmes de virement bancaire à distance par Internet prévoient d'habitude que l'ordre de virement soit exécuté le jour même s'il est passé un jour ouvré et avant une heure limite, sinon l'exécution interviendra le jour suivant. Ces systèmes permettent aussi les ordres de virement à exécution différée lesquels peuvent alors être révoqués jusqu'à la veille de la date d'exécution demandée[82].

Les conditions générales d'Odysseo, le portefeuille virtuel de BLUE LINE International qui est une société française, ne comportent pas non plus de clause d'irrévocabilité ou, au moins, d'exécution immédiate. Elles indiquent que le débit du porte-monnaie (la partie du portefeuille qui fonctionne comme un compte virtuel prépayé) sera effectué à la date indiquée sur chaque « *ticket de caisse* »[83].

115 Pourtant, la Recommandation communautaire du 30 juillet 1997, concernant les opérations effectuées au moyen d'instruments de paiement électronique, demande que les ordres de paiement donnés au moyen d'un instrument de paiement électronique soient irrévocables.

116 Comme nous venons de le montrer, la France traite le problème de l'irrévocabilité de l'ordre de paiement sur Internet de façon inégale pour les différents moyens de paiement. L'usage des cartes de paiement est soumis à une irrévocabilité absolue, tant dis que les ordres donnés par d'autres moyens sont révocables. Une telle disparité n'est pas en phase avec les intentions de la Commission européenne qui promeut actuellement une approche cohérente à perspective pro-consumériste de l'irrévocabilité de l'ordre de paiement.

CHAPITRE 2

L'approche cohérente à perspective pro-consumériste

117 Avant d'arriver au point d'équilibre que nous appelons ici « l'approche cohérente à perspective pro-consumériste », la position de la Commission européenne à l'égard de l'irrévocabilité de l'ordre de paiement a subi une évolution. De l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte de paiement, soutenue par exemple dans la recommandation du 8 décembre 1987[84], elle a évolué vers l'irrévocabilité presque absolue de tous les ordres de paiement. Cette position a été exprimée pour la dernière fois dans la

[82] Voir par exemple la Convention BNP Net, article 7.2, disponible sur www.bnpnet.bnp.fr/html/f_conv.htm .
[83] Les conditions générales d'Odysseo sont disponibles sur www.odysseo.com .
[84] JOCE 24 déc. 1987, n° L 365, p. 72.

recommandation du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique. Récemment, la Commission européenne a été amenée à changer cette approche en admettant les bénéfices de la procédure de remboursement pour les consommateurs.

Ainsi, nous décrirons d'abord l'approche rigoureuse de la recommandation de 1997 (section 1). Ensuite, nous étudierons la procédure de remboursement (section 2) qui introduit les exceptions pro-consuméristes dans le principe de l'irrévocabilité de l'ordre de paiement.

Section 1

L'approche rigoureuse de la recommandation de 1997

118 La recommandation n° 97/489/CE du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique traite la question de l'irrévocabilité des ordres de paiement dans son considérant 10 et à l'article 5. La réponse qu'elle apporte est très concise. Elle établit l'irrévocabilité générale des ordres de paiement (§ 1.). Mais, comme il s'agit d'un texte dépourvu du caractère contraignant, la mise en œuvre de ce principe dans les droits nationaux n'est pas partout aboutie (§ 2.).

§ 1. L'irrévocabilité générale des ordres de paiement

119 La recommandation prévoit dans le considérant 10 que « sans préjudice des droits éventuellement accordés au titulaire par le droit national, les instructions de paiement données par le titulaire dans les opérations qu'il réalise au moyen d'un instrument de paiement électronique doivent être irrévocables, à l'exception de celles dont le montant n'est pas connu au moment où l'instruction est donnée ». Nous retrouvons une disposition similaire à l'article 5 relatif aux obligations du titulaire, or cette fois sans mention des droits éventuellement accordés au titulaire. L'article 5 s'exprime aussi d'une façon plus elliptique, car il prévoit l'irrévocabilité d'une « instruction qu'il [le titulaire] a donnée au moyen de son instrument de paiement électronique ».

Le texte couvre alors les ordres de paiement (nommés instruction de paiement) donnés au moyen de tous les instruments de paiement électronique. D'après la recommandation, l'instrument de paiement électronique[85] est un terme générique qui englobe, d'une part, les instruments de paiement d'accès à distance et, de l'autre part, les instruments de monnaie électronique.

120 Nous devons remarquer qu'il serait plus approprié de restreindre de principe d'irrévocabilité des ordres de paiement aux seuls instruments de paiement d'accès à distance. En fait, ce sont les seuls moyens de paiement[86] qui fonctionnent à base des ordres de paiement. Les instruments de monnaie électronique constituent les moyens de paiement

[85] Défini à l'article 2, a) de la recommandation.

[86] Les moyens de paiement tels que définis par l'article L. 311-3 du Code monétaire et financier.

avec les unités de valeur stockées.

L'instrument de paiement d'accès à distance est défini à l'article 2, b) comme « un instrument permettant à son détenteur d'avoir accès aux fonds détenus sur son compte auprès d'un établissement et qui autorise, moyennant généralement la réalisation d'un code d'identification personnel et/ou la production de toute autre preuve d'identité similaire, la réalisation de paiements à un bénéficiaire ». Il s'agit alors des cartes de paiement ou des différents moyens de paiement qui s'y rattachent, comme l'envoie du numéro d'identification de la carte, l'emploi des numéros sécurisés, la communication de la volonté de payer par une carte choisie parmi celles répertoriées chez l'intermédiaire ; les applications de banque par Internet et celles des comptes virtuels rentrent aussi dans la définition.

121 Ainsi, tous les ordres de paiement donnés par ces moyens de paiement doivent être irrévocables, à une exception près. Les ordres de paiement de montants initialement inconnus sont au contraire reconnus révocables. De telles situations ne sont pas nombreuses après la transposition de l'article 4 de la directive du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance, qui oblige à fournir l'information sur le prix du bien ou service, toutes taxes comprises, avant la conclusion du contrat.

§ 2. La transposition dans les droits nationaux

122 La Commission européenne a récemment publié une étude réalisée en 2000-2001 sur la conformité de la législation des 15 États membres avec la recommandation précitée[87]. Notons que cette étude était prévue par le considérant 12 de la recommandation où la Commission exprime son intention de proposer une législation contraignante si elle juge les résultats de la mise en œuvre de la recommandation insatisfaisants. En général, l'étude a relevé que la recommandation a été très peu prise en considération[88]. Il sera intéressant de suivre l'activité de la Commission car le secteur bancaire semble être toujours fortement opposé à l'adoption d'une directive.

123 D'après les conclusions de l'étude, le principe d'irrévocabilité des ordres de paiement est affirmé la plupart du temps au niveau des contrats. C'est le cas du Danemark, de l'Autriche, l'Allemagne, la Belgique et la Grèce. L'Espagne et le Luxembourg ont consacré l'irrévocabilité des ordres de paiement dans leurs législations. En Irelande et en Italie, l'irrévocabilité n'est pas prévue[89].

En ce qui concerne l'exception au principe d'irrévocabilité pour les opérations dont le montant n'est pas connu au moment de la passation de l'ordre, les termes des contrats ne mentionnent pas cette exception ou stipulent expressément l'irrévocabilité[90].

---

[87] « Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment intruments and in particular the relationship between holder and issuer », Final Report, 20 mars 2001, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.htm .

[88] A. SALAÜN, « Étude européenne : le points sur la position des 15 à l'égard des instruments de paiement électronique », disponible sur www.droit.fundp.ac.be/textes/etude%20paiements.pdf .

[89] L'étude précitée, Final Report – part a), p. 76.

[90] Ibid., p. 78.

124 L'approche de la recommandation communautaire tendant à l'irrévocabilité de tous les ordres de paiement paraît parfaitement justifiée dans son principe. Mais n'y a-t-il pas de situations où une exception pro-consumériste pourrait être légitime ? Si nous revenons encore une fois au considérant 10 de la recommandation, nous nous apercevons que l'irrévocabilité est exigée « sans préjudice des droits éventuellement accordés au titulaire par le droit national ». Cela pourrait signifier que dans certains cas spécifiques, le donneur d'ordre aurait le droit de révoquer son ordre régulièrement donné.

La Commission européenne s'engage depuis quelques mois dans cette voie. Elle prévoit de mettre en place un cadre législatif communautaire garantissant le droit au remboursement en cas de problèmes surgissant entre le donneur d'ordre et le commerçant[91].

Section 2

La procédure de remboursement

125 Aujourd'hui, la procédure de remboursement n'est législativement consacrée que dans certains pays et même là, il ne s'agit pas d'un système d'application générale. Elle est liée à l'utilisation des cartes de crédit. Elle permet de régler les différends survenant entre le titulaire de la carte et le fournisseur à travers le réseau des émetteurs de cartes. L'éventail des cas où le remboursement est permis s'étend au-delà des ordres de paiement réguliers. Les États, comme la France, qui ne connaissent pas d'exception à l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte, utilisent cette procédure en cas d'ordres frauduleux. Mais c'est une autre histoire qui sera abordée plus loin[92].

126 En comparant les résultats du commerce électronique aux États-Unis et en Europe, la Commission européenne a compris l'importance de la procédure de remboursement pour le renforcement de la confiance des consommateurs. D'après l'exemple américain, elle prétend l'instaurer en Europe.

Nous étudierons d'abord la réglementation des États-Unis – la source d'inspiration (§ 1.). Ensuite, nous présenterons rapidement la situation actuelle en Europe (§ 2.) et enfin, la vision de la Commission européenne (§ 3.).

§ 1. La réglementation des États-Unis : la source d'inspiration

127 La procédure de remboursement aux États-Unis est régie par un certain nombre de lois fédérales et de lois des États. Dans les cas prévus, ils accordent au titulaire de la carte de crédit le droit au remboursement. Cette procédure est fondée sur le principe de la responsabilité solidaire du prêteur, donc de l'émetteur de la carte de crédit. Au niveau

[91] Communication de la Commission européenne « Commerce électronique et services financiers », COM (2001) 66 final du 7 février 2001, p. 18, disponible sur http://europa.eu.int/comm/internal_market/fr/finances/general/ecomfaq.htm .

[92] Voir le titre 2 de la seconde partie.

fédéral, la procédure de remboursement est régie par le Truth in Lending Act (TILA) et le Règlement Z qui est un règlement d'application du TILA.

128 Le Règlement Z instaure une procédure de « résolution des erreurs de facturation » (Billing error resolution)[93]. Cette procédure s'applique, entre autres, aux cas où les biens ou les services n'ont pas été acceptés par le consommateur ou aux cas où les biens ou les services n'ont pas été livrés comme prévu. Dans ces situations, la société de cartes de crédit est obligée d'ouvrir une enquête à la suite d'une réclamation du titulaire. La réclamation peut être introduite dans les 60 jours qui suivent la date du premier relevé. L'émetteur doit accuser réception de la réclamation et régler le litige dans un délai de deux cycles de facturation ou dans les 90 jours, si ce délai est plus court. Il doit procéder à une « enquête appropriée », c'est-à-dire se tourner vers le commerçant pour obtenir des informations. Le commerçant doit les fournir dans un délai précis. Si, à la suite de l'enquête, l'émetteur considère qu'une erreur est survenue, il crédite le compte du titulaire de la carte. Dans le cas contraire, il envoie une explication au titulaire donnant les raisons pour lesquelles il conclut à la régularité de la transaction fondamentale.

129 Le Règlement Z connaît encore une procédure dont l'application est plus restreinte. L'article (section) 226.12 (c) permet de régler par le réseau des émetteurs de carte certains différends ayant trait à la qualité des biens et des services ou à des produits défectueux. Le Règlement pose quelques conditions restrictives : l'opération contestée doit porter sur un montant supérieur à 50 dollars, le titulaire de la carte ne doit pas verser le montant contesté avant la procédure, la transaction doit être effectuée sur le territoire de l'État du titulaire de la carte ou à 100 milles au plus de l'adresse postale du titulaire de la carte. Ces conditions remplies, le titulaire de la carte qui a fait un effort raisonnable pour résoudre le différend avec le commerçant peut utiliser les moyens de défense qui découlent de la transaction contestée auprès de l'émetteur. Si le litige est réglé en faveur du titulaire de la carte, l'émetteur de la carte doit créditer son compte du montant contesté, sans autre frais.

130 Alors, nous pouvons constater que, dans certains cas, la législation des États-Unis permet au donneur d'ordre de paiement de révoquer son ordre. Pourtant l'irrévocabilité est toujours le principe et toutes les exceptions au principe doivent être au préalable justifiées. Nous remarquons encore que la révocation de l'ordre de paiement peut dans une des procédures citées survenir même après l'exécution de l'ordre.

La situation actuelle en Europe est en général différente.

§ 2. La situation actuelle en Europe

131 En Europe, seuls le Royaume-Uni, le Danemark, la Finlande et la Suède connaissent le principe de la responsabilité solidaire du prêteur - émetteur de la carte de crédit. Ce principe s'applique dans des circonstances qui diffèrent légèrement d'un pays à l'autre[94].

132 La procédure de remboursement n'est pourtant pas inconnue dans d'autres pays. Elle est prévue par les réglementations internes des sociétés de cartes de paiement. Or, comme il s'agit de l'autorégulation, il n'existe pas d'harmonisation de ces procédures internes. Elles diffèrent parmi les réseaux des émetteurs de cartes. Leur application à la transaction

[93] Section 226.13, disponible sur www.cardreport.com/laws/tila/tila2.html#226.12 .
[94] « Le recours du consommateur dans un marché international : les remboursements », OECD/GD(96)142, p. 57, disponible sur www.oecd.org//dsti/sti/it/consumer/prod/f_96-142.pdf .

est d'ailleurs très variable parce qu'elle dépend du droit national, des dispositions du contrat entre émetteur de la carte et le titulaire et des règles entre les membres du réseau.

Le point le plus important est que ces réglementations internes n'accordent pas aux titulaires de la carte le droit au remboursement. C'est l'émetteur qui décide si la réclamation du titulaire de la carte est acceptée.

133 Dans les pays où l'irrévocabilité des ordres de paiement donnés au moyen d'une carte est prévue pour les transactions nationales, les titulaires de carte de paiement ne sont pas forcément informés de l'existence de telles procédures de remboursement. Ils ne penseront pas à se tourner vers l'émetteur si un problème se révèle dans la transaction réglée à l'aide de la carte[95]. Quant aux émetteurs, ils n'ont pas envie de faire publicité à la procédure de remboursement parce qu'ils craignent les abus de ce mécanisme qui s'avère pour eux assez cher.

La Commission européenne considère cette situation insatisfaisante car elle nuit à la généralisation de la procédure de remboursement dont l'effet est bénéfique.

§ 3. La vision de la Commission européenne

134 La procédure de remboursement a des opposants et des défenseurs, mais son bénéfice pour le consommateur est évident. Elle le dispense de la nécessité d'intenter le procès judiciaire qui n'est pas un remède accessible pour le consommateur si le différend surgit à propos d'une transaction transfrontalière à distance. La pratique des remboursements montre qu'ils sont capables de renforcer la confiance des consommateurs dans le commerce électronique[96]. Il paraît que l'une des raisons du décalage entre les résultats du commerce électronique aux États-Unis et en Europe est justement l'absence des exceptions de l'irrévocabilité des ordres de paiement donnés au moyen d'une carte de paiement.

135 Dorénavant, la Commission européenne peut être comptée parmi les défenseurs des remboursements. Dans sa communication du 7 février 2001, elle affirme qu'il est « urgent de mettre en place, au niveau communautaire, un cadre législatif instituant un droit au remboursement en cas de transaction non autorisée ou de non-livraison et précisant les conditions à ce remboursement »[97]. Elle préconise aussi les mesures non législatives qui définiraient les objectifs et le cadre dans lequel le secteur pourra décider des modalités les plus appropriées pour s'acquitter de ses obligations.

136 En ce que concerne l'irrévocabilité de l'ordre de paiement, nous pouvons alors noter que la Commission est d'accord avec l'atténuation de ce principe en cas de non-livraison du produit ou service. Elle ne prévoit pas d'instaurer les remboursements pour les litiges portant sur la qualité.

Nous ne savons pas avec certitude si la Commission entend introduire cette exception à

---

[95] « Payment card chargeback when paying over Internet », First Sub-group meeting of the PSTDG and PSULG held on 4 July 2000, document MARKT/173/2000, p. 5, disponible sur http://europa.eu.int .

[96] R. PICHLER, « Finality of Credit Card Payments and Consumer Confidence – Different Approches in the United States and in Europe », *ePSO Newsletter*, n° 5, février 2001, disponible sur www.epso.jrc.es . Voir du même auteur « Trust and Reliance – Enforcement and Compliance : Enhancing Consumer Confidence in the Electronic Marketplace », thèse Standford University, mai 2000, disponible sur www.law.standford.edu/library/special/rufus.thesis.pdf .

[97] Communication de la Commission européenne « Commerce électronique et services financiers », COM (2001) 66 final du 7 février 2001, p. 19, disponible sur http://europa.eu.int/comm/internal_market/fr/finances/general/ecomfaq.htm .

l'irrévocabilité des ordres de paiement généralement pour tous les ordres de paiement sans égard pour le moyen de paiement utilisé ou si, plus classiquement, elle ne veut l'appliquer qu'aux ordres donnés au moyen de cartes de crédit. De toute façon, la communication de la Commission emploie des termes généraux et ne semble pas distinguer d'après les différents instruments de paiement.

137 Si les positions concernant l'irrévocabilité de l'ordre de paiement sur Internet sont encore parfois incohérentes, comme nous l'avons montré dans l'exemple français, la Commission européenne semble trouver la voie médiane. Elle consacre le principe de l'irrévocabilité de tout ordre de paiement, mais toutefois entend imposer l'instauration de quelques exceptions à ce principe justifiées par la position des consommateurs dans les systèmes de paiement.

Nous pouvons conclure cette partie en énonçant que, durant ces dernières années, les concepts permettant de soutenir l'efficacité de l'ordre de paiement sur Internet ont été élaborés. Le soutien de l'efficacité de l'ordre de paiement sur Internet a été quelquefois le résultat de mesures plus générales, comme dans le cas de la consécration de la signature électronique. D'autres fois, les mesures prises visaient expressément l'ordre de paiement sur Internet, comme le montre l'activité de la Commission européenne.

Bien entendu, l'efficacité de l'ordre de paiement ne concerne que l'ordre de paiement régulier. Les ordres de paiement frauduleux ne doivent pas non seulement bénéficier de cette efficacité, mais ils doivent supprimer. Cela nous mène alors à l'étude, dans notre seconde partie, de la suppression de l'ordre de paiement frauduleux sur Internet.

SECONDE PARTIE

La suppression de l'ordre de paiement frauduleux sur Internet

138 L'ordre de paiement frauduleux sur Internet constitue un problème grave qui va en s'accroissant. La principale cause de fraude est l'utilisation du numéro d'identification de la carte bancaire pour ordonner le paiement sur Internet. Mais il ne faut pas négliger l'existence des ordres de paiement frauduleux donnés par les moyens de paiement sécurisés. La sécurité des systèmes de paiement n'est jamais absolue, l'affaire Serge Humpich en témoigne[98].

139 Le poids exact des pertes résultant des ordres de paiement frauduleux sur Internet est difficile à évaluer. En France, les seules statistiques précises existent pour les cartes bancaires émises dans les conditions fixées par le Groupement des cartes bancaires « CB ». Les données statistiques représentent en plus une agrégation des déclarations de fraude fournies par toutes les banques. Cela veut dire que ces informations ne prennent pas en compte les pertes dues à la fraude qui ne sont pas supportées par les banques. Or, il est fort possible que le poids des pertes dues à la fraude supportées par les commerçants ou les consommateurs est plus élevé que celui des pertes supportées par les banques.

140 La hausse de la fraude entre 1999 et 2000 est sensible pour l'ensemble des opérations par carte. En ce qui concerne les paiements frauduleux, leur volume a augmenté de 40%[99]. Les pertes dues aux paiements frauduleux par carte en France ont été chiffrées à hauteur de 250 millions de francs[100]. Vu l'approche restrictive de ces statistiques, nous pouvons penser que les données sont fortement sous-estimées. Le domaine de la fraude la plus répandue est celui où le paiement est déclenché par les ordres de paiement sur Internet donnés au moyen de l'envoie du numéro de la carte. Presque 50% des contestations des

---

[98] L'affaire a été fortement médiatisée. Il s'agissait d'un informaticien qui a percé le « secret » de la carte à puce. Il a été condamné le 25 février 2000 par la 13e chambre correctionnelle du Tribunal de grande instance de Paris pour la contrefaçon ou falsification de cartes de paiement ou de retrait, pour l'accès et maintien frauduleux dans de système de traitement automatisé de données, pour l'introduction frauduleuse de données dans un système de traitement automatisé et pour l'usage de cartes de paiement ou de retrait contrefaites ou falsifiées. Voir T. corr. Paris, 25 février 2000, *D.* 2000, Jur., p. 219, obs. X. Delpech ; *RDBF*, mai/juin 2000, p. 165, obs. E. A. Caprioli.

[99] Avis de M. Jean-Pierre BRARD, au nom de la commission des finances, n° 2992, du 18 avril 2001, disponible sur www.assemblee-nationale.fr .

[100] M. JASOR, « Forte progression de la fraude à la carte bancaire dans les paiements à distance », *Les Échos*, 24 et25 novembre 2000, p. 1 et 36.

ordres de paiement relèvent de ce domaine[101] et les pertes à la suite de ces contestations sont, d'après les contrats entre les émetteurs de cartes et les commerçants, supportées par les commerçants.

141 Pour effectuer un ordre de paiement sur Internet, il est indispensable de disposer des données permettant d'ordonner le paiement. Afin de prévenir les ordres de paiement frauduleux sur Internet, ces données doivent être protégées. Cela nous mènera à étudier, dans un premier temps, la protection des données permettant d'ordonner le paiement sur Internet. Lorsque ces mesures de protection se montrent insuffisantes, car un ordre de paiement frauduleux est pourtant survenu, la personne autorisée à disposer des fonds qui ont été transférés à cause de la fraude, doit pouvoir se défendre. Ainsi, dans un second temps, nous analyserons les possibilités de défense de l'ayant droit contre les ordres de paiement frauduleux sur Internet.

TITRE 1

La protection des données permettant d'ordonner le paiement sur Internet

142 En relation avec les ordres de paiement sur Internet, la protection des données permettant d'ordonner le paiement devient particulièrement importante. À cause du caractère ouvert et international d'Internet, le flux des données transitant par le réseau et pouvant être exploitées frauduleusement est considérable. Le stockage même des données sur les serveurs des commerçants et des intermédiaires financiers peut s'avérer vulnérable. Les numéros d'identification et les dates d'échéance des cartes de paiement, qui n'étaient pas à l'origine conçues comme les données permettant d'ordonner le paiement, peuvent être facilement capturés hors réseau et réutilisés sur Internet.

Il est alors évident que la suppression des ordres de paiement frauduleux sur Internet demande une relative confidentialité des données permettant d'ordonner le paiement. Dans le chapitre 1, nous verrons les mesures utilisées à ces fins par la pratique. Mais, l'efficacité de ces mesures pratiques ne pouvant pas se concevoir sans le concours du droit, nous exposerons la protection juridique dans le chapitre 2.

[101] « Payment card chargeback when paying over Internet », First Sub-group meeting of the PSTDG and PSULG held on 4 July 2000, document MARKT/173/2000, p. 4, disponible sur http://europa.eu.int .

CHAPITRE 1

Les mesures utilisées dans la pratique

143 Parmi les mesures pratiques qui contribuent à la protection des données permettant d'ordonner le paiement sur Internet, la cryptographie utilisée aux fins confidentielles constitue peut-être la mesure la plus importante (section 1). Mais d'autres procédés assurant la confidentialité participent aussi activement à la lutte contre les ordres de paiement frauduleux sur Internet (section 2).

Section 1

La cryptographie aux fins confidentielles

144 La cryptographie[102], étant le procédé qui consiste en la transformation des données en une forme inintelligible et dans l'opération inverse, peut servir à régler de multiples situations. Comme nous l'avons vu plus haut, elle permet l'authentification et la vérification de l'intégrité des données. Mais son rôle principal est d'assurer la confidentialité des données et, partant, de sécuriser leurs transmission et stockage.

Premièrement, nous décrirons le fonctionnement technique de la cryptographie utilisée aux fins confidentielles (§ 1.). Deuxièmement, l'encadrement juridique de la cryptographie sera présenté (§ 2.) car dans le cas de la France, la cryptographie n'est pas soumise à l'heure actuelle à un régime libéralisé.

§ 1. Le fonctionnement technique

145 La confidentialité des données permettant d'ordonner le paiement sur Internet peut être assurée de deux façons différentes. La première fait l'usage de la cryptographie symétrique (A.), la seconde de la cryptographie asymétrique (B.).

A. La cryptographie symétrique

146 La protection des données par la cryptographie symétrique est basée sur l'utilisation d'une clé cryptographique secrète. La clé secrète constitue un instrument renfermant un algorithme mathématique qui est capable de transformer des données, de manière à les rendre inintelligibles par quiconque ne possède pas cette clé. La clé cryptographique est alors unique ; elle sert pour chiffrer et déchiffrer les données.

[102] D'autres termes peuvent être utilisés à la place de cryptographie, par exemple le cryptage, la cryptologie ou le chiffrement. La terminologie n'étant pas fixée, il faut tenir toutes ces notions pour équivalentes.

147 La cryptographie symétrique peut être employée pour chiffrer les données stockées telles que les codes confidentiels ou les numéros d'identification des cartes. Si elle devait assister à la protection du transport des même données par le réseau, la communication de la clé secrète commune pourrait s'avérer problématique.

En effet, la communication de la clé à l'autre partie doit se faire par un moyen assurant la non-interception de la clé par des tiers. Ainsi, la clé devrait être communiquée hors réseau. Ce problème peut être facilement résolu par le recours à la cryptographie asymétrique.

B. La cryptographie asymétrique

148 La cryptographie asymétrique, autrement dit la cryptographie à clé publique, est apparue dans les années soixante-dix. En 1976, W. DIFFIE et H. HELLMAN ont présenté dans une œuvre intitulée « Multiuser cryptographic Techniques » le concept de la cryptographie à clé publique qui permet à des parties d'échanger des données chiffrées sans avoir à se communiquer par avance une clé secrète commune[103]. Comme nous l'avons décrit plus haut, le système met en œuvre une paire de clés, l'une privée, qui est tenue secrète, et l'autre publique, qui est révélée au public.

Si le message est chiffré avec la clé publique du destinataire, il ne peut être déchiffré qu'avec sa clé privée. Ainsi, la confidentialité du message est assurée. En effet, il s'agit de l'inversement des fonctions des clés par rapport à la signature électronique où la clé privée est utilisée pour chiffrer le message et la clé publique pour le déchiffrer.

La première application de la cryptographie asymétrique largement déployée vient de R. RIVEST, A. SHAMIR et L. ADLEMAN qui l'ont inventée en 1978. Ce système, appelé RSA du nom de ces auteurs, est le représentant du type exponentiel des crypto-systèmes. Il est basé sur les nombres premiers. Il existe encore deux familles plus jeunes des crypto-systèmes, les systèmes de logarithme divisé et les systèmes de cryptographie à courbes elliptiques.

149 En relation avec les ordres de paiement sur Internet, la cryptographie asymétrique est mise en œuvre grâce au protocole SSL ou au protocole SET. Le protocole SSL (Secure Socket Layer) est un protocole de communication, c'est-à-dire qu'il n'est pas limité aux cas d'ordres de paiement et il a vocation à s'appliquer aussi aux différentes transmissions de données. Il met en œuvre le crypto-système RSA. La sécurisation des données de l'ordre de paiement par le protocole SSL est la plus répandue des méthodes de sécurisation sur Internet. Cela est dû à son intégration dans le « Netscape Navigator » et le « Microsoft Internet Explorer ».

Sous le protocole SSL, la communication sécurisée commence par l'interconnexion entre le logiciel client et le logiciel serveur de type commercial[104]. À ce moment là, le logiciel serveur possède déjà sa paire de clés. Le logiciel client génère une paire de clés dont la clé publique est ensuite fournie au logiciel serveur. Toutes les données transmises après entre le client et le serveur commercial seront chiffrées grâce à ces deux paires de clés. Ainsi, la confidentialité de la communication est assurée, mais le serveur commercial

---

[103] A. McCULLAGH, W. CAELLI, P. LITTLE, « Signature Stripping : A Digital Dilemma », *The Journal of Information, Law and Technology (JILT)*, http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html . Récemment, il a été découvert que la cryptographie à clé publique avait été développée par le service secret GCHC du Royaume-Uni déjà au début des années soixante-dix.

[104] BAITAN, BERGER, MAIA, « Le protocole SSL (Secure Socket Layer) », 22 mai 1998, disponible sur www.esigge.ch/reche98/protoSSL/SSL.htm .

ne peut pas vérifier l'identité de l'utilisateur du logiciel client. Pour cette raison, les sociétés de cartes de paiement ont encouragé le développement du protocole SET.

150 Le protocole SET (Secure Electronic Transaction) est un protocole exclusivement conçu pour le paiement par carte via Internet[105]. Il a été développé conjointement par Visa International et MasterCard dès 1996. Ce protocole utilise en même temps la cryptographie symétrique et asymétrique. L'ordre de paiement est chiffré à l'aide d'une clé cryptographique symétrique générée au hasard[106]. Cette clé est ensuite elle-même chiffrée par la clé publique du destinataire, ce qui est connu sous le nom d'enveloppe digitale. Cette enveloppe digitale est envoyée avec l'ordre de paiement chiffré. Le destinataire déchiffre premièrement l'enveloppe digitale avec sa clé privée. Deuxièmement, il déchiffre l'ordre de paiement avec la clé symétrique ainsi obtenue.

Comme nous l'avons étudié auparavant, le protocole SET met aussi en œuvre la signature électronique ce qui permet de vérifier l'imputabilité de l'ordre de paiement au donneur d'ordre. La fonction de signature électronique est également assurée par la cryptographie asymétrique. Mais le protocole SET utilise pour cela une autre paire de clés cryptographiques que celle servant à la création de l'enveloppe digitale. De ce fait, chaque participant au système SET possède deux paires de clés asymétriques, l'une de « clés d'échange » pour chiffrer et déchiffrer l'ordre de paiement, et l'autre de « clés de signature » pour la création et la vérification de la signature numérique.

151 Nous avons vu que la cryptographie rend techniquement possible la confidentialité des données permettant d'ordonner le paiement sur Internet. Or, le droit a quelquefois restreint cette possibilité technique.

§ 2. L'encadrement juridique

152 La cryptographie était historiquement employée pour les applications liées à la défense et à la sécurité nationale. Cela explique son encadrement assez strict par le droit de certains pays, par exemple la France. Mais l'expansion du commerce électronique et du paiement sur Internet demande un accès plus facile à la cryptographie.

À l'heure actuelle, la réglementation française traduit encore la conception ancienne, bien qu'atténuée (A.), c'est pourquoi un projet de loi sur la société de l'information tend à libéraliser le régime de la cryptographie (B.).

A. La réglementation française actuelle

153 La réglementation touchant la cryptographie en France est issue de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications. Cet article a été modifié par la loi n° 96-659 du 26 juillet 1996 qui a entamé le processus de

[105] D. BOUNIE et L. VANINETTI, « E-payments : Which Systems in Europe for the Comming Years ? », *STAR Issue Report* n° 13, juin 2001, p. 7, disponible sur www.databank.it/star/list_issue/g.html après l'inscription.

[106] « SET Secure Electronic Transaction Specification, Book 1 : Business Description », p. 18, disponible sur www.setco.org/download/set_bk1.pdf .

libéralisation de la cryptographie. Le législateur a choisi le terme de cryptologie pour désigner ce que nous appelons dans notre développement la cryptographie[107].

154 Selon l'article 28 de la loi, il faut distinguer l'utilisation d'un moyen ou d'une prestation de cryptologie de leurs fourniture, importation et exportation[108]. Quant à l'utilisation du moyen ou de la prestation de cryptologie, la loi différencie son régime d'après les fonctions que ce moyen ou cette prestation peuvent remplir. Lorsque la fonction de confidentialité peut être atteinte, la loi se montre plus sévère. Dans ce cas là, elle permet l'utilisation du moyen ou de la prestation de cryptologie sans aucune formalité seulement à condition que le moyen ou la prestation n'utilisent que des conventions secrètes gérées selon les procédures et par un organisme agrées dans les conditions définies par la loi. Si tel n'est pas le cas, l'utilisation est soumise à l'autorisation préalable du Premier ministre. En ce qui concerne la fourniture, l'importation et l'exportation des moyens ou prestations de cryptologie assurant la confidentialité, la loi les soumet également à l'autorisation préalable du Premier ministre.

155 Cependant, la loi prévoit des simplifications que les décrets peuvent mettre en place. Cela est possible dans la situation où il ne peut pas être porté atteinte aux intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État. Par le décret n° 99-200 du 17 mars 1999, certaines catégories de moyens et de prestations de cryptologie ont été dispensées de toute formalité préalable. Le décret n° 99-199 de la même date a substitué pour certaines catégories la procédure de déclaration préalable à la procédure d'autorisation.

Les décrets sont construits sous forme de tableaux : ils énumèrent les procédés techniques dans la première colonne et dans la seconde, ils précisent pour chaque procédé laquelle des opérations d'utilisation, de fourniture, d'importation ou d'exportation bénéficie du régime allégé.

156 Pour le stockage des données permettant d'ordonner le paiement sur Internet, le point 10 du tableau du décret n° 99-200 est important. Il dispense dans une large mesure des formalités préalables les opérations d'utilisation, d'exportation et d'importation qui concernent les procédés chiffrant les fichiers de codes confidentiels utilisés pour contrôler l'accès aux services de paiement. De manière plus générale, l'utilisation et l'importation des procédés cryptographiques sont libres si la clé cryptographique n'excède une certaine longueur de bits. La longueur est fixée à 40 bits et elle peut monter jusqu'à 128 bits à condition que les procédés soient destinés à l'usage privé d'une personne physique.

157 Bien que l'utilisation de la cryptographie aux fins confidentielles soit assurée dans une certaine mesure par la réglementation actuelle, le gouvernement français, habité par le souhait de renforcer la confiance dans les nouvelles technologies, a décidé le 19 janvier 1999 la libéralisation totale de l'utilisation de la cryptographie. Ce même but a été finalement intégré dans le projet de loi sur la société de l'information.

---

[107] Nous avons préféré le terme de cryptographie car le suffixe « –logie » de la notion de cryptologie est employé dans un sens impropre ; il ne s'agit pas ici d'une science.

[108] En simplifiant, le moyen de cryptologie désigne un matériel ou logiciel dont l'objectif est de transformer les informations intelligibles en inintelligibles ou inversement. La prestation de cryptologie est définie comme prestation visant le même objectif.

B. Le projet de loi sur la société de l'information

158 Dans son titre V, le projet de loi sur la société de l'information[109] instaure un nouveau régime plus libéral de la cryptographie. Il assouplit grandement les modalités de contrôle des moyens de cryptologie par rapport aux dispositions des décrets n° 99-199 et 99-200 du 17 mars 1999.

159 Le projet de loi libère entièrement l'utilisation de tous les moyens de cryptologie[110]. Le régime de la fourniture, du transfert depuis un État membre de la Communauté européenne ou de l'importation des moyens qui assurent la fonction de confidentialité sera soumis à la déclaration préalable auprès du Premier ministre. Par contre, le transfert des même moyens vers un État membre de la Communauté européenne et leur exportation sont soumis à l'autorisation du Premier ministre.

Comme à l'état actuel, le projet prévoit l'allégement du régime par décret. Si les caractéristiques techniques ou les conditions d'utilisation sont telles qu'elles ne nuisent pas aux intérêts de la défense nationale et de la sécurité intérieure de l'État, le transfert vers un État membre de la Communauté européenne ou l'exportation peuvent être soumis soit à la déclaration préalable, soit dispensés de toute formalité.

160 Ainsi, nous pouvons prévoir que la liberté étendue par le projet de loi sur la société de l'information contribuera au renforcement de la protection des données permettant d'ordonner le paiement sur Internet. L'emploi des clés cryptographiques ayant une longueur plus importante ne sera plus soumis à des formalités qui peuvent s'avérer lourdes et entraver les transactions sur Internet.

161 Bien que la cryptographie, que nous venons d'étudier, représente une mesure primordiale pour la protection de la confidentialité des données, d'autres procédés peuvent venir conforter cette protection de la confidentialité.

Section 2

D'autres procédés assurant la confidentialité

162 Ces dernières années ont vu apparaître des procédés moins radicaux que la cryptographie assurant la confidentialité des données permettant d'ordonner le paiement sur Internet. Ils ne garantissent pas la confidentialité des données stockées, ce qui représentent le domaine de prédilection de la cryptographie, mais ils sont efficaces dans la protection des données susceptibles d'utilisation frauduleuse car ils empêchent leur circulation sur le réseau.

La circulation des données sur le réseau peut être évitée par la meilleure protection des

[109] Document n° 3143 du 18 juin 2001, disponible sur www.assemblee-nationale.fr .

[110] La définition de moyen de cryptologie est d'ailleurs remaniée pour qu'elle corresponde mieux à l'existence de la cryptographie asymétrique. Cette dernière n'est pas bien prise en compte par la loi du 29 décembre 1990 qui ne vise que les conventions secrètes comme l'outil de chiffrement et donc omet les clés publiques de la cryptographie asymétrique.

données hors ligne. Ainsi, nous décrirons premièrement l'aménagement des facturettes (§ 1.). La protection en ligne est néanmoins possible. Nous serons alors amenés à étudier deuxièmement la circulation des données périssables (§ 2.).

§ 1. L'aménagement des facturettes

163 Les données apparentes des cartes de paiement n'étaient pas à l'origine conçue comme des données permettant à elles seules d'ordonner le paiement. Avec l'avènement du commerce par la communication dématérialisée à distance, tel que le commerce par téléphone ou sur Internet, les données apparentes des cartes de paiement sont devenues les éléments suffisants pour ordonner le paiement.

Pourtant, la simple utilisation d'une carte de paiement hors ligne contribue à la diffusion des données apparentes. Le titulaire de la carte n'est pas lui-même capable de garder les données apparentes confidentielles. Certaines techniques de fraude sont donc relativement simples à mettre en œuvre. Les données nécessaires pour les ordres de paiement sont relevées sur les facturettes des pointes de vente ou des distributeurs automatiques de billets.

Il ne s'agit pas d'une délinquance sans importance. Par exemple, en février 2000, la branche française d'un groupe de fraudeurs ivoiriens a été démantelée[111]. Ils utilisaient le réseau Internet de leur cité universitaire pour commander des montres de luxe et des billets d'avion à l'aide des numéros de cartes relevés dans les grands hôtels d'Abidjan.

164 Il est alors opportun de prévoir des aménagements des facturettes sur lesquelles les données nécessaires peuvent être récupérées. C'est pour cela que le 22 février 2001, le Conseil du Commerce de France s'est engagé à recommander à ses adhérents la mise en œuvre des modifications de la facturette du porteur de la carte de paiement pour la fin de l'année 2001[112]. Il a été prévu que seront supprimés l'identité du porteur, le numéro d'autorisation et la date de fin de validité. Surtout, les numéros d'identification des cartes de paiement devront être tronqués. Le dispositif est déjà mis en œuvre par certains, mais sa seule application généralisée réduira la fraude relative à la « découverte » des données permettant d'ordonner le paiement.

165 Un autre système de protection des données susceptibles de réutilisation frauduleuse se met déjà en place sur Internet même. Il consiste en la circulation des données périssables.

§ 2. La circulation des données périssables

166 Les ordres de paiement donnés au moyen de l'envoi du numéro apparent et la date d'expiration inscrits sur la carte de paiement représentent la majorité des ordres de paiement sur Internet. Afin de maintenir ce système, il a été imaginé d'octroyer un numéro d'identification et une date d'expiration pour une transaction unique dans le but de ne pas

[111] Avis de M. Jean-Pierre BRARD, au nom de la commission des finances, n° 2992, du 18 avril 2001, disponible sur www.assemblee-nationale.fr .

[112] Il s'agit de l'une des deux chartes signées le même jour, relatives à la sécurité des cartes de paiement. La charte est disponible sur www.afb.fr/securitecarte.htm .

divulguer la véritable identité de la carte de paiement. Ces données périssables sont connues sous le nom de numéros sécurisés.

167 Nous avons déjà brièvement présenté les solutions basées sur ce système. Les numéros sécurisés peuvent être émis, après l'enregistrement du titulaire de la carte, par le logiciel qu'il télécharge ou qui est implanté sur le serveur de l'émetteur de la carte. Le titulaire de la carte s'identifie par un procédé définit par l'émetteur. Le logiciel crée au hasard un numéro unique à la transaction qui est ensuite associé au compte du titulaire. Une date d'expiration unique, souvent très courte, est adjointe à ce numéro. Ces données sont communiquées au titulaire de la carte qui les utilise de façon habituelle pour remplir le formulaire d'un commerçant sur Internet.

Ainsi, les données qui sont envoyées par Internet ne permettent pas d'ordonner un autre paiement que pour lequel elles étaient issues. Les fonds du titulaire sont donc mieux protégés contre la fraude.

168 Nous avons vu que la pratique a su imaginer plusieurs procédés techniques tendant à la protection des données permettant d'ordonner le paiement sur Internet. En sus, le droit a complété les procédés pratiques.

CHAPITRE 2

La protection juridique

169 Le droit est intervenu pour créer des obligations à l'égard de ceux qui traitent les données permettant d'ordonner le paiement. C'est pour cela que nous allons étudier en premier lieu la protection des données à caractère personnel (section 1).

Le législateur a également mis en place des mesures répressives contre ceux qui se livrent à des agissements frauduleux. Nous serons en second lieu amener à analyser ces mesures réprimant la fraude relative aux données (section 2).

Section 1

La protection des données à caractère personnel

170 À partir des années soixante-dix, certains États européens, parmi lesquels la France, se sont peu à peu dotés de cadres législatifs relatifs à la protection des données à caractère personnel. Ce cadre législatif est applicable aux données permettant d'ordonner le paiement sur Internet. Ainsi, le concept de la protection législative des données à caractère personnel sera détaillé dans un premier temps.

Étant donné que le réseau Internet est de toute évidence un réseau de communication international et qu'un certain nombre d'États, dont les États-Unis, ne partagent pas la conception européenne de la protection des données à caractère personnel, il est indispensable de promouvoir une protection à travers l'autorégulation. Dans un second temps, nous présenterons alors cette protection à travers l'autorégulation.

§ 1. La protection législative des données à caractère personnel

171 Avec le développement du traitement automatisé des données, la législation relative à la protection des données à caractère personnel est apparue dans certains pays européens. L'exemple de l'Allemagne et de la Suède[113] a été bientôt suivi par l'adoption en France de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ces législations ont été mises en place surtout dans le but de protéger les particuliers contre les possibles dérives de l'Administration qui avait le potentiel de concentrer un nombre important de données à caractère personnel. Cette préoccupation du législateur se reflète dans la loi française car elle distingue entre le traitement à caractère public et privé des données.

172 Cette distinction n'a plus lieu d'être aujourd'hui car avec le développement des microinformatiques dans le secteur privé, les dangers pouvant découler du traitement automatique des données se sont étendus à ce secteur. C'est pourquoi la directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, a consacré une réglementation applicable aux secteurs public et privé sans distinction. Cette directive sera bientôt transposée dans le droit français. Un projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-18 du 6 janvier 1978[114] a été finalement élaboré et enregistré à la Présidence de l'Assemblée nationale le 18 juillet 2001. La France aura finalement rempli l'obligation de transposition de la directive après trois ans de retard.

173 Les données permettant d'ordonner le paiement sur Internet, telles que les numéros d'identification des cartes de paiement et les codes confidentiels, entrent dans le champ d'application de la loi française et de la directive communautaire. Elles sont couvertes par la définition d'informations nominatives[115] incluse dans la loi, de même que par la définition de données à caractère personnel[116] du projet de la loi transposant la directive 95/46/CE. Ainsi, les personnes responsables d'un traitement des données permettant d'ordonner le paiement sur Internet doivent se conformer à cette législation.

Le projet de loi a vocation à s'appliquer au traitement des données à caractère personnel dont le responsable est établi sur le territoire français ou dont le responsable recourt à des moyens de traitement sur le territoire français. Cela veut dire que même

---

[113] C. CHASSIGNEUX, « La protection des données personnelles en France », *Lex Electronica*, vol. 6, n° 2, hiver 2001, n° 10, www.lex-electronica.org/articles/v6-2/chassigneux.htm .

[114] Document n° 3250 du 18 juillet 2001, disponible sur www.assemblee-nationale.fr .

[115] En vertu de l'article 4, les informations nominatives sont celles qui permettent l'identification directe ou indirecte des personnes physiques auxquelles elles s'appliquent.

[116] Après l'adoption du projet de la loi, une nouvelle définition relative aux données à caractère personnel se trouvera à l'article 2 de la loi du 6 janvier 1978. Ladite définition vise toute information relative à une personne identifiée ou indentifiable.

l'emplacement en France d'un serveur étranger traitant les données à caractère personnel aura pour conséquence l'application de la législation française.

174 Parmi différentes obligations que le responsable du traitement doit assumer figure l'obligation de sécurité des opérations portant sur les données. Comme dans la rédaction actuelle[117], le projet de loi prévoit[118] que le responsable est tenu de prendre toutes précautions utiles pour empêcher notamment que les données ne soient communiquées à des tiers non autorisés. Le considérant 46 de la directive communautaire précise encore que les mesures adoptées par le responsable doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en œuvre.

Nous pouvons en déduire que les établissements de crédit, les prestataires de paiement sur Internet sont obligés de protéger les serveurs contenant les numéros des cartes de paiement ou les codes confidentiels par des mesures techniques habituelles, par exemple les pare-feu. Nous pouvons aussi supposer que les données stockées doivent être chiffrées. De plus, la directive exige la mise en œuvre de certaines mesures d'organisation qui devraient protéger les données par exemple contre l'accès non autorisé.

175 En cas de non-respect des dispositions légales, le responsable du traitement des données à caractère personnel devra répondre de ses insuffisances. D'une part, sa responsabilité délictuelle pourra être engagée et il sera contraint à verser des dommages et intérêts. Il est intéressant d'observer que le projet de loi modifiant la loi du 6 janvier 1978 ne suit pas exactement les dispositions de la directive 95/46/CE. En effet, il découle de l'article 23, alinéa 2 de la directive que la faute du responsable du traitement est présumée. Sa responsabilité devrait être engagée dans tous les cas où il n'arrive pas à prouver que le fait qui a provoqué le dommage ne lui est pas imputable. Or le projet de loi ne contient aucune disposition spécifique sur la responsabilité[119], d'où il est nécessaire de conclure que la responsabilité du responsable du traitement sera fondée sur les articles 1382 et 1383 du Code civil et donc la faute devra être prouvée par l'endommagé.

D'autre part, si des poursuites sont engagées, le responsable du traitement pourra être sanctionné administrativement ou pénalement. Les sanctions pénales concernant l'omission de l'obligation de sécurité se trouvent d'ores et déjà dans le Code pénal[120]. Contrairement à la situation actuelle, après l'adoption du projet de loi, la Commission nationale de l'informatique et des libertés pourra, après une procédure contradictoire et lorsqu'une mise en demeure préalable sera restée sans effet, prononcer des sanctions pécuniaires. En cas d'urgence, les mesures provisoires d'interruption du traitement ou de verrouillage de certaines données pourront être prononcées. Enfin, en cas d'atteinte grave et immédiate aux droits et libertés garantis par la loi, la commission pourra saisir le juge des référés.

176 Comme nous l'avons exposé, l'obligation légale de sécurité des données à caractère personnel mise en place par les États européens renforce la protection de la confidentialité des données permettant d'ordonner le paiement sur Internet. Mais, même les textes autonomes peuvent s'avérer efficaces à l'égard de cette protection.

---

[117] Art. 29 de la loi du 6 janvier 1978.
[118] Art. 5, section 1 du projet de la loi.
[119] Pourtant le rapport BRAIBANT prévoyait la transposition dudit article de la directive. Voir G. BRAIBANT, « Données personnelles et la société de l'information », rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998, p. 78, disponible sur www.ladocfrancaise.gouv.fr .
[120] Art. 226-17 du code pénal.

§ 2. La protection à travers l'autorégulation

177 L'autorégulation, ou autrement dit les textes autonomes, se rapporte « aux normes volontairement développées et acceptées par ceux qui prennent part à une activité »[121]. En relation avec la protection des données permettant d'ordonner le paiement sur Internet, l'autorégulation se traduit en l'élaboration de politiques de protection des données personnelles ou de codes de bonne conduite ou bien en la certification par labels. Ces approches autonomes sont d'autant plus importantes qu'Internet constitue un réseau international. En effet, les disparités entre les législations relatives à la protection des données à caractère personnel sont tellement grandes qu'elles pourraient empêcher d'établir la confiance des internautes dont les données personnelles seraient traitées. L'opposition frappante est surtout remarquée entre l'approche européenne, basée sur la réglementation législative, et la position américaine, préconisant l'autorégulation fondée sur l'idée de l'équilibrage automatique entre les intérêts des commerçants et des consommateurs[122].

178 En élaborant des politiques de protection des données personnelles, les responsables du traitement des données affichent clairement leurs méthodes de protection à l'usage des personnes dont les données sont traitées. En ce qui concerne la confidentialité des données permettant d'ordonner le paiement sur Internet, ces politiques énoncent d'habitude les mesures de sécurité mises en œuvre par le responsable du traitement.

179 Parmi les politiques de protections des données personnelles se trouvent les codes de bonne conduite qui constituent, en fait, des politiques de protection harmonisées pour un certain secteur. Il s'agit d'un procédé issu de la culture juridique anglo-saxonne qui a été repris comme une méthode subsidiaire de régulation par les droits européens. Depuis un certain temps, le législateur communautaire prend en compte ces codes de bonne conduite et incite à leur élaboration. La directive 95/46/CE comporte une disposition dans ce sens à l'article 27. Elle oblige les États à encourager l'élaboration des codes. L'alinéa 2 prévoit également que de tels codes pourront être soumis à l'examen de l'autorité nationale. Enfin, même les projets de codes communautaires sont prévus.

Le projet de loi modifiant la loi du 6 janvier 1978 effectue la transposition de l'article 27, alinéa 2 de la directive. À la demande des organismes professionnels, la Commission nationale de l'informatique et des libertés (CNIL) pourra donner son avis sur la conformité aux dispositions de la loi des projets de codes de bonne conduite. Le projet de loi, comme la directive, ne dit rien sur la valeur juridique et la force contraignante des codes de bonne conduite. En l'absence de disposition relative aux conséquences de non-respect de tels codes, nous pouvons conclure qu'il ne sera pas possible d'infliger les sanctions administratives ou pénales aux commettants d'infraction aux codes.

180 Quant à la certification par label, il s'agit d'un procédé qui combine la technologie et l'audit[123]. Il consiste à apposer sur le site un label qui garantira le respect de certains engagements. La labellisation est étroitement liée au développement des codes de conduite,

---

[121] Conseil d'État, « Internet et les réseaux numériques », note 8, p. 3, disponible sur http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm .

[122] G. BRAIBANT, « Données personnelles et la société de l'information », rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998, p. 94, disponible sur www.ladocfrancaise.gouv.fr .

[123] D. GOBERT et A. SALAÜN, « La labellisation des sites web : Classification, stratégies et recommandations », *Droit et Nouvelles technologies*, dossier du 20 février 2000, p. 2, disponible sur www.droit-technologie.org, .

car ceux-ci peuvent servir de base aux critères que les sites s'engagent à respecter[124]. Sur Internet, il existe plusieurs certificateurs qui délivrent les labels après s'être assurés du respect des mesures protégeant les données à caractère personnel. Nous pouvons citer par exemple L@belsite, un certificateur français[125].

181 Bien que l'autorégulation ne soit pas obligatoire, elle peut renforcer la protection des données à caractère personnel et, dans notre cas, assurer la confidentialité des données permettant d'ordonner le paiement sur Internet. Les consommateurs s'orientent en fonction des labels et des codes de bonne conduite attribués aux sites ce qui incite les responsables du traitement des données à se soumettre à l'autorégulation.

182 La protection juridique des données permettant d'ordonner le paiement sur Internet ne demande pas seulement la réglementation de l'activité de ceux qui traitent ces données. Il est indispensable de dissuader la fraude relative à ces données.

Section 2

Les mesures réprimant la fraude relative aux données

183 Pour la protection des données permettant d'ordonner le paiement sur Internet, il est essentiel d'incriminer pénalement les agissements des tiers qui accèdent ou utilisent frauduleusement ces données. Les fraudeurs peuvent forcer les mesures techniques mises en place par les responsables du traitement des données, bien que ces derniers aient assumé toutes leurs obligations. L'incrimination pénale de la fraude relative aux données doit alors jouer un rôle préventif par ses sanctions lourdes.

Les organes internationaux et communautaires, conscients du développement de la cyber-criminalité, ont pris certaines initiatives adressées aux États pour qu'ils se préoccupent de ce phénomène (§ 1.). Après la présentation de ces initiatives, nous nous intéresserons à l'état du droit pénal en France (§ 2.).

§ 1. Les initiatives internationales et communautaires

184 Au niveau international et communautaire, la nécessité de lutter efficacement contre la criminalité informatique a été largement reconnue[126]. Diverses organisations internationales, telles que l'Organisation des Nations-Unies, l'Organisation de coopération

[124] Op. cit., p. 3.

[125] Pour d'autres exemples de certificateurs présents sur le marché, voir C. CHASSIGNEUX, « La protection des données personnelles en France », *Lex Electronica*, vol. 6, n° 2, hiver 2001, n° 51, www.lex-electronica.org/articles/v6-2/chassigneux.htm .

[126] Communication de la Commission européenne « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cyber-criminalité », COM(2000) 890 final du 26 janvier 2001, p. 7, disponible sur http://europa.eu.int .

et de développement économique ou le Conseil de l'Europe, et la Commission européenne ont entrepris des actions dans ce domaine.

Ces actions sont nées à cause des disparités importantes entre les législations nationales. En effet, avec le développement de la cyber-criminalité, certains États ont commencé à légiférer contre cette criminalité sans qu'un consensus international n'ait été recherché. D'autres États n'ont pris aucune disposition spécifique en la matière.

185 Le Conseil de l'Europe a commencé en février 1997 à élaborer une convention internationale sur la criminalité informatique et devrait avoir achevé ses travaux en 2001. Parmi les infractions retenues par le projet de la convention figurent, entre autres, les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques et les infractions informatiques. Le projet final[127] de la convention a été adopté par le Comité européen pour les Problèmes Criminels lors de sa 50e session plénière du 18 au 22 juin 2001. Il attend d'être présenté au Comité des Ministres pour son adoption.

186 Quant à l'Union européenne, elle a lancé un certain nombre de mesures ne relevant pas du domaine législatif. En 1998, la communication intitulée « Un cadre d'action pour lutter contre la fraude et la contrefaçon des moyens de paiement autre que les espèces » a été publiée[128]. Le projet de l'action commune, contenu à l'annexe de cette communication, est devenu, à la suite des changements opérés par le traité d'Amsterdam, une proposition de décison-cadre[129]. La décision-cadre proposée a été compétée par la communication du 9 février 2001[130].

187 L'objectif de la proposition de la décision-cadre est l'incrimination de toute fraude impliquant un moyen de paiement autre que les espèces. Les États membres sont invités, par l'article 3, à l'adoption des textes qui érigeront en infractions pénales les actes délictueux référencés à l'article 2 de la proposition. Parmi ces actes délictueux, nous trouvons aussi l'utilisation non autorisée, en connaissance de cause, de données d'identification pour le lancement ou le traitement d'une opération de paiement. Cette disposition concerne donc l'utilisation frauduleuse des données permettant d'ordonner le paiement sur Internet.

188 La décision-cadre ne concerne pas le simple accès non-autorisé à un système de paiement utilisant la technologie de l'information, mais pourtant, elle mentionne expressément la faculté des États membres de l'incriminer. C'est ce que le droit pénal français connaît depuis la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dont les dispositions ont été codifiées dans le nouveau Code pénal.

---

[127] Le projet final de la Convention sur la cyber-criminalité est disponible sur http://conventions.coe.int/Treaty/FR/cadreprojets.htm .

[98] Communication de la Commission européenne « Un cadre d'action pour lutter contre la fraude et la contrefaçon des moyens de paiement autres que les espèces », COM (1998) 395 final, disponible sur http://europa.eu.int .

[129] Proposition de décision-cadre du Conseil visant à combattre la fraude et la contrefaçon des moyens de paiement autres que les espèces, COM (1999) 438 final du 14 septembre 1999, disponible sur http://europa.eu.int .

[130] Communication de la Commission européenne « Prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces », COM (2001) 11, p. 8, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11fr.pdf .

§ 2. L'état du droit pénal en France

189 Le droit pénal français permet de sanctionner la fraude relative aux données permettant d'ordonner le paiement sur Internet. L'accès ou le maintien illicite aux bases automatisées de ces données est réprimé par des dispositions spécifiques du Code pénal concernant les atteintes aux systèmes de traitement automatisé de données. Par contre, l'utilisation frauduleuse de ces données pour ordonner le paiement sur Internet relève des dispositions plus générales du Code pénal.

190 L'accès ou le maintien illicite dans les bases de données est l'un des moyens possibles de se procurer les données permettant d'ordonner le paiement sur Internet. Ces agissements sont couverts par l'article 323-1 du Code pénal. Celui-ci s'applique à l'accès ou au maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données. Le Code ne donne pas de définition du système de traitement automatisé de données, mais il est évident qu'une base de données automatisée correspond à la définition. Le délinquant encourt dans ce cas un an d'emprisonnement et 100 000 F d'amende.

191 L'incrimination de l'utilisation frauduleuse de données permettant d'ordonner le paiement sur Internet, comme l'exige la proposition de la décision-cadre sus-mentionnée, n'est pas réalisée de façon spécifique en France. Cette situation peut mener à des doutes quant à la qualification de l'infraction. L'hésitation est permise entre le vol ou l'escroquerie[131]. De notre part, il nous semble que le délit d'escroquerie est le mieux approprié. En effet, l'utilisation frauduleuse de données détermine l'établissement de crédit ou le prestataire de paiement sur Internet, par l'emploi de manœuvres frauduleuses, à remettre des fonds au préjudice de la personne autorisée à disposer de ces fonds. Ce fait entre alors bien dans la définition de l'escroquerie de l'article 313-1 du Code pénal.

192 Nous avons montré que la pratique a imaginé des mesures permettant la protection des données servant à ordonner le paiement sur Internet, par exemple la cryptographie. Le législateur a concouru à cette tâche en instaurant le dispositif relatif aux données à caractère personnel et en incriminant les agissements frauduleux. Même si ces mesures tendant à la protection des données permettant d'ordonner le paiement sur Internet sont mises en place, des ordres de paiement frauduleux peuvent encore survenir. Pour ces situations, des possibilités de défense de l'ayant droit contre les ordres de paiement frauduleux doivent être prévues.

[131] Lamy Droit du financement, *Cartes de paiement et de crédit*, n° 2434, Éditions Lamy 2001.

TITRE 2

Les possibilités de défense de l'ayant droit contre les ordres de paiement frauduleux sur Internet

193 Les ordres de paiement frauduleux ne sont pas des ordres de paiement valides. Toutefois, il est impossible de les distinguer des ordres réguliers parce qu'ils abusent des moyens de paiement de la personne autorisée à disposer des fonds sur un compte. C'est alors le titulaire du moyen de paiement lui-même qui doit se défendre contre l'exécution des ordres de paiement frauduleux par l'émetteur - teneur de son compte.

194 En cas de perte, de vol ou d'utilisation frauduleuse du moyen de paiement, le titulaire doit disposer d'un moyen pour prévenir l'émetteur du risque d'ordres frauduleux et de solliciter l'interdiction d'exécuter les ordres de paiement et l'invalidation du moyen de paiement en question. Dans ces situations, la défense du titulaire sera assurée par l'opposition[132] à l'exécution des ordres frauduleux.

Suivant la thèse que le titulaire du moyen de paiement ne doit pas supporter les risques dus à l'insécurité du système de paiement, le titulaire doit pouvoir déplacer sur l'émetteur les pertes subies à cause de l'exécution d'un ordre de paiement frauduleux survenu sans que le titulaire ait pu supposer la fraude. Dans de cas pareils, le titulaire aura recours à la demande en annulation du paiement.

Nous devons remarquer que ces deux possibilités de défense contre les ordres frauduleux ne sont pas nécessairement exclusives l'une de l'autre. Ainsi, il faut distinguer le cas de perte ou de vol du moyen de paiement (chapitre 1) et les cas d'utilisation frauduleuse sans dépossession du moyen de paiement (chapitre 2) où la demande d'annulation du paiement et l'opposition doivent souvent se combiner.

CHAPITRE 1

La perte ou le vol du moyen de paiement

195 La perte ou le vol ne concernent que les moyens de paiement matériels. En relation avec les ordres de paiement sur Internet, nous pouvons nous limiter à l'étude de la défense du titulaire contre les ordres frauduleux donnés au moyen d'une carte de paiement perdue ou volée. La défense en cas de perte ou de vol de la carte passe par la procédure d'opposition.

[132] Nous employons le terme « opposition » qui est utilisé par le Code monétaire et financier français en relation avec la carte, bien qu'il soit peu clair car se trouvant dans le Code dans divers contextes. Le terme « notification » de la recommandation communautaire n° 97-489 et des règlements américains désigne la déclaration de perte ou de vol, ce que le Code, une fois le projet de loi sur la sécurité quotidienne adopté, l'appellera « mise en opposition ».

196 En France, le régime juridique de l'opposition en cas de perte ou de vol dépend actuellement du contrat conclu entre l'émetteur et le titulaire de la carte. La seule disposition législative concernant l'opposition se trouve à l'article L. 132-2, deuxième phrase du Code monétaire et financier et elle ne précise pas son régime juridique. Cette situation changera après l'adoption par le Parlement du projet de loi relative à la sécurité quotidienne dont le chapitre III vise à modifier le Code monétaire et financier.

Aux États-Unis, le régime juridique de l'opposition est depuis longtemps régi par la législation. Ce régime s'avère très protecteur des consommateurs. La Commission européenne, guidée par la même volonté de protection des consommateurs, a dressé le régime juridique qu'elle souhaiterait donner à l'opposition en cas de perte ou de vol à l'article 6, paragraphes 1 et 2 de la recommandation n°97-489 concernant les opérations effectuées au moyen d'instruments de paiement électronique.

Ces différents textes sur l'opposition en cas de perte ou de vol précisent les obligations du titulaire de la carte et de l'émetteur dans la procédure d'opposition (section 1). Ensuite, ils opèrent le partage des pertes dues à l'exécution des ordres frauduleux (section 2).

Section 1

Les obligations dans la procédure d'opposition

197 Pour que le mécanisme de l'opposition puisse bien fonctionner et par la suite devenir le moyen de défense efficace du titulaire contre les ordres frauduleux donnés au moyen d'une carte perdue ou volée, l'émetteur et le titulaire doivent assumer les obligations qui leur incombent dans cette procédure. Nous verrons d'abord les obligations de l'émetteur (§ 1.), puis nous décrirons celles du titulaire (§ 2.).

§ 1. Les obligations de l'émetteur

198 L'émetteur doit premièrement fournir au titulaire les moyens lui permettant d'effectuer la mise en opposition, c'est-à-dire la déclaration de perte ou de vol de la carte. Cette obligation est mentionnée à l'article 5, paragraphe 2, d) et à l'article 9, paragraphe 1 de la recommandation communautaire du 30 juillet avec la précision que ce service doit être accessible vingt-quatre heures sur vingt-quatre. La récente étude sur la transposition de la recommandation dans les droits des États membres de l'Union européenne a relevé qu'en Grande Bretagne et au Portugal cette obligation figure dans les lois. Les émetteurs français et finnois respectent cette obligation, tant dis qu'en Autriche, la période de déclarations possibles est souvent restreinte aux heures d'ouverture. Aux Pays-Bas et en Italie, les contrats entre l'émetteur et le titulaire omettent la plupart du temps de mentionner les moyens de la mise en opposition[133].

[133] « Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment intruments and in particular the relationship between holder and issuer », Final Report,

199 Aux États-Unis, le règlement d'application du Truth in Lending Act (TILA), dit Règlement Z, prévoit que l'émetteur doit informer le titulaire de façon adéquate des moyens de la mise en opposition. Du point de vue de l'émetteur, cette obligation est essentielle. Si elle n'est pas respectée, l'émetteur doit supporter la totalité des pertes dues aux ordres frauduleux donnés par la carte de crédit perdue ou volée. Une disposition similaire se trouve à la section 205.6 (a) du Règlement E qui est un règlement d'application de « Electronic Fund Transfer Act » et dont le champ d'application couvre les autres cartes de paiement. Le Règlement E ajoute encore l'obligation d'informer des jours ouvrables ce qui implique que le service de mises en opposition peut ne pas fonctionner sans interruption.

200 La communication de la Commission européenne du 9 février 2001 relative à la prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces prévoit qu'un numéro de téléphone européen unique, gratuit et facile à mémoriser pourrait être créé[134]. À tout le moins, elle demande un numéro de téléphone unique valable pour tous les émetteurs de chaque État membre. La France dispose déjà d'un tel numéro[135].

Vu que les déclarations par téléphone peuvent être difficiles à prouver, la recommandation communautaire demande à l'article 5 précité que l'émetteur fournisse au titulaire les moyens de preuve qu'il a effectué la déclaration. L'étude de la transposition de la recommandation indique que les émetteurs fournissant les moyens de preuve de la déclaration téléphonique sont rares[136]. Un bon exemple est Card Stop belge qui donne un numéro permettant de prouver la date et l'heure de la déclaration[137].

201 Une autre obligation de l'émetteur, qui explique l'importance de l'opposition pour le titulaire, se trouve à l'article 9, paragraphe 2 de la recommandation communautaire. Cet alinéa prévoit que l'émetteur est tenu, dès la déclaration, même si le titulaire a agi avec une négligence extrême ou de manière frauduleuse, de faire tout ce qui est raisonnablement en son pouvoir pour empêcher toute nouvelle utilisation de l'instrument de paiement électronique. En effet, la carte doit être inscrite sur une liste qui est, entre autre, consultable par les commerçants qui peuvent ainsi refuser d'accepter les ordres de paiement frauduleux. D'habitude, les textes ne contiennent pas cette obligation de l'émetteur car son exécution paraît être dans l'intérêt de l'émetteur qui doit supporter les pertes résultant des ordres de paiement frauduleux après la mise en opposition. Or, dans le cas où le commerçant n'aurait pas le paiement garanti, ce qui est fréquent pour les transactions sur Internet, les pertes se répercutent sur le commerçant mais pas sur l'émetteur. C'est pour cela qu'il est plus qu'opportun de mentionner cette obligation dans les textes. En France, l'obligation est reconnue par la jurisprudence[138].

La disposition précitée apporte implicitement le principe selon lequel l'émetteur n'a pas à se faire juge de la validité de l'opposition.

---

20 mars 2001, p. 80, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.htm .

[134] Communication de la Commission européenne « Prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces », COM (2001) 11, p. 8, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11fr.pdf .

[135] Avis de M. Jean-Pierre BRARD, au nom de la commission des finances, n° 2992, du 18 avril 2001, disponible sur www.assemblee-nationale.fr .

[136] « Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment intruments and in particular the relationship between holder and issuer », Final Report précité, 20 mars 2001, p. 80.

[137] A. SALAÜN, « Étude européenne : le points sur la position des 15 à l'égard des instruments de paiement électronique », disponible sur www.droit.fundp.ac.be/textes/etude%20paiements.pdf .

[138] Voir par exemple Cass. com., 20 oct. 1998, *JCP* éd. E 1999, p. 1101, note J. Devèze.

§ 2. Les obligations du titulaire de la carte

202 Si le titulaire de la carte perdue ou volée veut se défendre effectivement contre les éventuels ordres de paiement frauduleux, il doit déclarer la perte ou le vol de la carte dans un certain délai à l'émetteur. Le non-respect de cette obligation a des incidences négatives pour le titulaire en ce qui concerne le partage des pertes.

Différentes conceptions de ces délais existent. La recommandation communautaire du 30 juillet 1997 ne prévoit pas un délai précis. D'après l'article 5, b), le titulaire est obligé de notifier à l'émetteur la perte ou le vol dès qu'il en a connaissance.

Le Règlement E américain oblige le titulaire de faire la mise en opposition dans les deux jours ouvrables à compter du moment où il a eu connaissance de la perte ou du vol de la carte. C'est pour cela que l'émetteur est obligé d'informer le titulaire de ses jours ouvrables car ces « business days » peuvent être fixés librement par l'émetteur.

Le projet de loi relative à la sécurité quotidienne, qui devrait être adopté par le Parlement français en automne 2001, opère une harmonisation partielle des délais de la mise en opposition. L'article 7 *ter* prévoit que la mise en opposition doit être faite dans les meilleurs délais après la perte ou le vol de la carte, compte tenu des habitudes du titulaire d'utilisation de la carte de paiement. Le contrat entre l'émetteur et le titulaire peut prévoir un délai précis, mais il ne peut pas être inférieur à deux jours francs après la perte ou le vol. Ainsi, par rapport à la situation actuelle où le délai est souvent fixé par l'émetteur à 24 heures[139], le titulaire sera mieux protégé des pertes dues à l'exécution des ordres de paiement frauduleux.

Nous pouvons constater que la prise en compte des habitudes d'utilisation de la carte équivaut implicitement à l'approche américaine de la fixation du moment après lequel la mise en opposition doit être faite. Le titulaire devra effectuer la mise en opposition dès qu'il aura connaissance de la perte ou du vol de la carte.

203 À cause de la preuve problématique des mises en opposition téléphoniques, la plupart des émetteurs obligent encore les titulaires à confirmer la mise en opposition par écrit. En France, le contrat « Carte bancaire » impose cette confirmation dans son article 10 et ajoute qu'en cas de contestation sur l'opposition, l'opposition sera réputée avoir été effectuée à la date de la réception de la confirmation[140]. Une telle stipulation dans le contrat entre l'émetteur et le titulaire pourra être contraire à la loi si elle conteste les effets de la mise en opposition téléphonique effectuée antérieurement et dans les délais car le projet de loi ne distingue pas d'après la façon de mise en opposition. D'ailleurs, le 22 février 2001, les établissements de crédit émetteurs de cartes de paiement ont signé la « Charte relative à la sécurité des cartes de paiement »[141] où ils se sont engagés à accepter la mise en opposition d'une carte perdue ou volée dès le premier appel sans obligation de communiquer le numéro de la carte, cela avant la fin du premier semestre 2001. Ainsi, la jurisprudence

---

[139] Rapport de M. Bruno LE ROUX, au nom de la commission des lois, n° 3177, du 26 juin 2001, disponible sur www.assemblee-nationale.fr .

[140] Pour l'application de ce contrat type, voir par exemple les « Dispositions générales de banque – clientèle des professionnels » du Crédit Lyonnais, disponible sur www.professionnels.creditlyonnais.com/info/pdf/dgb.pdf , qui contiennent cette clause à la page 13 : « Sauf preuve contraire, l'opposition est réputée avoir été effectuée à la date de réception par l'agence de ladite confirmation écrite. » Nous remarquons qu'ici, la preuve contraire est possible. Or, comme c'est l'obligation de l'émetteur de fournir au titulaire le moyen de preuve et le titulaire n'a pas la possibilité de se le procurer sans la coopération de l'émetteur, la clause fait subir sur le titulaire les conséquences de non-exécution de l'obligation de l'émetteur et donc, l'acceptation de l'opposition téléphonique est entièrement dans les mains de l'émetteur.

[141] La charte est disponible sur www.afb.fr/securitecarte.htm .

considérant les mises en opposition téléphoniques non confirmées par écrit comme irrégulières sera définitivement de l'histoire ancienne[142].

Aux États-Unis, le Règlement E prévoit expressément que le titulaire doit effectuer la mise en opposition personnellement, par téléphone ou par écrit. La mise en opposition est considérée faite peu importe si elle est effectuée auprès d'un service particulier ou non de l'émetteur.

204 L'exécution de ces différentes obligations de l'émetteur et le titulaire de la carte perdue ou volée influence de manière décisive le partage des pertes dues à l'exécution des ordres de paiement frauduleux.

Section 2

Le partage des pertes dues à l'exécution des ordres frauduleux

205 L'institution d'opposition en cas de perte ou de vol de la carte de paiement est bâtie sur le partage des pertes dues à l'exécution des ordres de paiement frauduleux. En effet, le titulaire a l'obligation d'assurer la sécurité de la carte[143]. C'est pour cette raison qu'il supporte en partie les pertes si sa carte est perdue ou volée, il est présumé partiellement responsable d'avoir permis la fraude. Mais dès qu'il effectue la mise en opposition et donc permet par cette information à l'émetteur d'empêcher l'exécution d'autres ordres frauduleux, l'attribution des pertes change.

Ainsi, nous étudierons consécutivement l'attribution des pertes avant la mise en opposition (§ 1.) et l'attribution des pertes après la mise en opposition (§ 2.).

§ 1. L'attribution des pertes avant la mise en opposition

206 Les textes réglementant l'opposition en cas de perte ou de vol de la carte laissent soit la partie, soit la totalité des pertes dues à l'exécution des ordres frauduleux à la charge du titulaire. Ils diffèrent dans les critères qui déterminent si la charge des pertes est plafonnée et dans la hauteur du plafond.

207 D'après le Règlement E américain, si la mise en opposition a été effectuée dans le délai de deux jours ouvrables déjà mentionné plus haut, le titulaire supporte les pertes dans la limite de 50 $. Si le titulaire n'a pas respecté le délai prévu pour la mise en opposition, les pertes à sa charge sont égales à 500 $ ou bien à 50 $ ou moins pour les pertes des deux premiers jours ouvrables plus le montant des pertes des jours suivants jusqu'au jour de la mise en opposition pourvu qu'il soit établi par l'émetteur que ces pertes ne seraient pas survenues si la mise en opposition avait été effectuée dans le délai. La réglementation

[142] Par exemple Cass. com., 1er mars 1994, *Bull. civ.* IV, n° 82, p. 63.
[143] Voir l'article 3 du contrat « Carte bancaire ».

américaine est aussi intéressante par le fait qu'elle protège totalement le titulaire contre la charge des pertes s'il n'a pas été informé des moyens de la mise en opposition.

208 La recommandation de la Commission européenne concernant les opérations effectuées au moyen d'instruments de paiement électronique prévoit le plafond des pertes à la charge du titulaire à 150 €. Ce plafond n'est pas applicable si le titulaire a agi avec une négligence extrême ou frauduleusement. La négligence extrême se rapporte à l'obligation du titulaire d'assurer la sécurité de la carte de paiement et du code confidentiel et à l'obligation de faire une mise en opposition dès qu'il a connaissance de la perte ou du vol de la carte.

209 En France, à l'heure actuelle, le régime du partage des pertes ne résulte pas d'un texte législatif ou réglementaire mais du contrat entre l'émetteur et le titulaire. Le contrat « Carte bancaire » distingue deux plafonds différents selon que l'opération donnant naissance à la perte nécessitait ou non le contrôle du code confidentiel. Si le contrôle était nécessaire, la charge des pertes pour le titulaire est limitée à 3 000 F ; dans le cas contraire, le plafond est fixé à 600 F. Or, le contrat comporte aussi les critères qui, s'ils sont remplis, mènent à l'attribution intégrale des pertes au titulaire. Il s'agit des cas de faute, imprudence ou opposition tardive, utilisation par le titulaire ou un membre de sa famille.

210 Si nous comparons la situation actuelle du titulaire d'après les contrats français à celle prévue par le règlement américain et à celle que la recommandation communautaire juge équitable, nous devons constater que la charge des pertes pesant sur le titulaire français est assez lourde. Premièrement, les plafonds sont fixés beaucoup plus haut que les autres textes le prévoient. Deuxièmement, les critères qui rendent ces plafonds inapplicables peuvent être facilement remplis. Le délai de la mise en opposition fixé par les émetteurs français est d'habitude de 24 heures. Après, il s'agit de l'opposition tardive. L'imprudence du titulaire est souvent retenue. Donc, fréquemment, le titulaire devra supporter toutes les pertes dues à l'exécution des ordres de paiement frauduleux avant la mise en opposition.

211 Le projet de loi relatif à la sécurité quotidienne changera cette situation. Le plafond des pertes supportées par le titulaire sera initialement fixé à 400 € et puis successivement abaissé jusqu'au plafond prévu par la recommandation communautaire, c'est-à-dire à 150 €. Le titulaire pourra supporter l'intégralité des pertes survenues avant la mise en opposition s'il agit avec une négligence constituant une faute lourde ou s'il n'effectue pas la mise en opposition dans les délais. Ces délais seront rallongés, comme nous l'avons précisé plus haut.

§ 2. L'attribution des pertes après la mise en opposition

212 Le principe de l'attribution des pertes après la mise en opposition est très simple. Le titulaire n'a plus à supporter les pertes consécutives à la perte ou le vol de la carte.
Cela vaut bien sûr seulement pour les cas où le titulaire de la carte n'a pas agi frauduleusement lui-même. C'est ce que la recommandation communautaire rappelle à l'article 6, paragraphe 2. Le contrat « Carte bancaire » l'exprime à l'article 11 où il décharge le titulaire des pertes résultant des opérations postérieures à la mise en opposition « à l'exception des opérations faites par lui [le titulaire] ».

Alors, après la mise en opposition, le titulaire de bonne foi qui a perdu ou s'est fait voler la carte ne peut plus souffrir de l'exécution des ordres de paiement frauduleux. Comme nous l'avons déjà relevé, la prise en charge par l'émetteur des éventuelles pertes après la mise en opposition dépendra de l'existence d'une garantie de paiement entre

l'émetteur et le commerçant. Si le commerçant n'a pas le paiement garanti, c'est alors lui qui supportera les conséquences néfastes de l'ordre de paiement frauduleux.

213 Nous avons vu qu'en cas de perte ou de vol du moyen de paiement, les pertes dues à l'exécution des ordres de paiement frauduleux sont partagées entre le titulaire et l'émetteur du moyen de paiement. Tel n'est pas le cas lorsqu'une utilisation frauduleuse sans dépossession du moyen de paiement survient.

CHAPITRE 2

L'utilisation frauduleuse sans dépossession du moyen de paiement

214 L'utilisation frauduleuse d'un moyen de paiement dont le titulaire n'est pourtant pas dépossédé peut être possible dans deux situations : soit un moyen de paiement immatériel a été divulgué ou découvert, soit un moyen de paiement matériel a été contrefait.

215 Le régime juridique de la défense du titulaire contre les ordres frauduleux en cas d'utilisation frauduleuse sans dépossession du moyen de paiement dépend de la sécurité du système de paiement. Nous étudierons d'abord le cas de système de paiement vulnérable (section 1). Ensuite, nous détaillerons le régime de la défense du titulaire dans le système de paiement sécurisé (section 2).

Section 1

Le système de paiement vulnérable

216 Nous entendons par système de paiement vulnérable celui qui ne dispose pas de procédé fiable d'identification du titulaire. Ainsi, l'utilisation frauduleuse du moyen de paiement par un tiers qui se l'est procuré à l'insu de son titulaire légitime est extrêmement facile.

Les solutions de paiement sur Internet les plus usuelles aujourd'hui sont justement celles qui utilisent un système de paiement vulnérable – l'envoi du numéro apparent d'identification de la carte de paiement.

Le régime juridique de la défense du titulaire contre les ordres frauduleux dans un tel système est basé sur une présomption d'utilisation frauduleuse du moyen de paiement par un tiers. La défense du titulaire est donc facilitée par le régime allégé d'annulation du paiement et de remboursement (§ 1.) et le régime allégé d'opposition (§ 2.).

§ 1. Le régime allégé d'annulation du paiement et de remboursement

217 Le titulaire d'un moyen de paiement ne doit pas supporter le poids des risques liés à la vulnérabilité du système de paiement. C'est un postulat largement accepté. Ainsi, le titulaire de la carte de paiement dont le numéro facial a été frauduleusement utilisé sur Internet doit pouvoir contester l'opération après en avoir pris connaissance.

218 La directive n° 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance[144] précise à l'article 8, relatif au paiement par carte, que « les États membres veillent à ce que des mesures appropriées existent pour que le consommateur : - puisse demander l'annulation d'un paiement en cas d'utilisation frauduleuse de sa carte de paiement dans le cadre de contrats à distance couverts par la présente directive, - en cas d'utilisation frauduleuse, soit recrédité des sommes versées en paiement ou se les voie restituées ».

219 En France, la situation actuelle, avant l'adoption de la loi relative à la sécurité quotidienne, est telle que le droit à l'annulation du paiement et au remboursement n'est pas affirmé au niveau législatif. En pratique, le titulaire a la possibilité de contester l'opération et d'être remboursé. Le contrat « Carte bancaire » permet, par l'article 13, les réclamations du titulaire et stipule qu'en cas de réclamation justifiée, la situation du compte sera restaurée. Alors, le contrat ne vise pas expressément l'annulation et le remboursement en cas d'utilisation frauduleuse de la carte mais ces procédures sont englobées dans le terme plus large de réclamation.

220 Lorsque le Code monétaire et financier sera modifié par la loi relative à la sécurité quotidienne, le régime d'annulation du paiement et de remboursement sera prévu par les articles L. 132-4 à L. 132-6. Le projet de loi, tel qu'adopté par l'Assemblée nationale en nouvelle lecture le 27 juin 2001, prévoit que si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de la carte, et le titulaire conteste par écrit de l'avoir effectuer, les sommes contestées lui sont recréditées sur son compte ou restituées, sans frais, au plus tard dans le délai d'un mois à compter de la réception de la contestation. Ensuite, il est prévu que l'émetteur doit rembourser aussi les frais bancaires que le titulaire a supporté à cause de l'opération contestée. L'article L. 132-6 ajoute finalement les délais dans lesquels l'opération frauduleuse peut être contestée. Le délai légal est fixé à soixante-dix jours à compter de l'opération contestée. Ce délai peut être prolongé contractuellement mais ne peut pas dépasser cent vingt jours à compter de l'opération.

Nous pouvons observer que le délai pour les contestations est rallongé par rapport à la situation actuelle où la version 7 du contrat « Carte bancaire » fixe le délai pour les réclamations à 120 jours maximum et de nombreux émetteurs adoptent alors le délai de 30 jours[145]. Le délai tel qu'il devrait figurer dans le Code monétaire et financier est plus long que le délai prévu par les Règlements Z et E américains qui obligent le titulaire à contester l'opération dans les 60 jours de l'envoi du relevé de compte. Par contre le délai accordé à l'émetteur pour le remboursement ne peut pas dépasser 10 jours à compter de la réception de la contestation aux États-Unis.

221 Les dispositions du projet de loi s'accordent avec les engagements pris par les établissements de crédit dans la « Charte relative à la sécurité des cartes de paiement » du 22 février 2001. En effet, la charte prévoit que les émetteurs inscriront dans le contrat

[144] Disponible sur http://europa.eu.int/eur-lex/fr/index.html .
[145] Avis de M. Jean-Pierre BRARD, au nom de la commission des finances, n° 2992, du 18 avril 2001, disponible sur www.assemblee-nationale.fr .

porteur le droit du titulaire de se faire rembourser les débits contestés de bonne foi liés à des achats à distance n'impliquant ni signature manuscrite, ni frappe du code confidentiel. Les émetteurs se sont encore engagés à rembourser en moins d'un mois les débits frauduleux liés à une contrefaçon de carte ou à une utilisation frauduleuse d'un numéro de carte. Une nouvelle version du contrat « Carte bancaire » doit être alors adoptée pour prendre en compte ces engagements qui, d'après la charte, devaient être accomplis avant la fin du premier semestre 2001.

222 Il faut insister sur le fait que les nouvelles dispositions du Code monétaire et financier apporteront une possibilité vraiment efficace de défense du titulaire. L'émetteur sera obligé par les dispositions du Code, et non plus seulement par la réglementation interne relative aux remboursements, de donner suite à la contestation du titulaire et de créditer son compte, tout cela sans nécessité pour le titulaire de prouver que le paiement contesté résulte d'un ordre de paiement frauduleux. Bien sûr, ce régime allégé d'annulation du paiement et de remboursement concernera seulement les cas où l'ordre de paiement a été donné à distance sans le contrôle physique de la carte, c'est-à-dire par l'envoi du numéro d'identification de la carte. La procédure est la même qu'en cas de remboursement pour d'autres causes[146], la seule différence dans cette situation où l'ordre de paiement a été donné par l'envoi du numéro apparent réside dans le fait que le commerçant, et partant l'émetteur, n'a aucune preuve que l'ordre de paiement est imputable au titulaire de la carte et donc l'annulation du paiement et le remboursement peuvent être prévus directement par la loi.

223 Le projet de loi sur la sécurité quotidienne prévoit le même régime d'annulation et de remboursement en cas de contrefaçon de la carte de paiement. Or est-il raisonnable de présumer la contrefaçon de la carte ? Nous pensons que pour l'annulation du paiement effectué selon un ordre donné au moyen d'une carte contrefaite, la contrefaçon, ou au moins la possibilité de contrefaçon, doit être prouvée. Mais ce n'est plus le même régime allégé d'annulation et de remboursement qu'en cas d'utilisation frauduleuse du numéro de la carte de paiement, ni le même régime allégé d'opposition.

§ 2. Le régime allégé d'opposition

224 La problématique d'opposition en cas l'utilisation frauduleuse du moyen de paiement est née d'une mauvaise disposition se trouvant à l'heure actuelle encore inchangée dans le Code monétaire et financier. Il s'agit de l'article L. 132-2 mentionné plus haut en relation avec l'irrévocabilité de l'ordre de paiement et la procédure d'opposition en cas de perte ou de vol de la carte de paiement. Cet article prévoit qu il « ne peut être fait opposition au paiement qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaires du bénéficiaire ».

Cette énumération des cas d'opposition, à tort limitative, a mené les émetteurs de cartes à ne pas accepter les oppositions en cas d'utilisation frauduleuse de la carte de paiement sans vol ou perte de la carte. Mais quelques décisions de justice et certains auteurs ont su écarter ce que le texte paraissait prévoir.

Pour contourner la malheureuse disposition, la jurisprudence a recouru au principe

[146] La réglementation américaine ne fait pas de différence entre les remboursements pour différentes causes et instaure une unique procédure. Voir Règlement E, section 205.11 Procedures for resolving errors, ou Règlement Z, section 226.13 Billing error resolution.

selon lequel l'émetteur n'a pas à se faire juge de la validité de l'opposition. Pour les oppositions en matière des cartes de paiement, ce principe n'est pas posé par la loi, mais son inobservation serait inacceptable.

225 La Cour d'appel d'Orléans a ainsi raisonné dans son arrêt du 2 février 1994[147]. En l'occurrence, Mme Pierre a loué un véhicule en laissant l'empreinte de sa carte bancaire. Ce véhicule a été détourné par un tiers contre lequel Mme Pierre a porté plainte pour vol et détournement après avoir effectué la mise en opposition de sa carte bancaire. La banque a pourtant débité le compte de Mme Pierre qui s'est ainsi trouvé débiteur. Puis, la banque a assigné Mme Pierre en paiement, à la suite de quoi a été rendue la décision confirmée par l'arrêt de la Cour d'appel d'Orléans. La cour, après avoir cité la disposition selon laquelle il ne peut être fait opposition qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaires du bénéficiaire, pose le principe sus-mentionné. Elle juge que la banque « n'avait pas à procéder à un paiement […] quel qu'ait pu être le véritable motif de l'opposition ».

226 Dans une autre affaire[148], la Cour de cassation a fait l'application du même principe, bien que l'exprimant différemment, en cassant et annulant l'arrêt de la Cour d'appel de Versailles entre les sociétés MAMI et American Express Carte France. Les faits dont cette affaire est issue étaient les suivants. La société MAMI a obtenu pour l'un de ses préposés à l'étranger, en se portant elle-même codébitrice solidaire, une carte accréditive de la société American Express. Or quelques mois plus tard, ce préposé a quitté l'entreprise et la société MAMI a demandé à l'émetteur l'annulation de la carte. American Express a pris acte de la demande, en réclamant la restitution de la carte et en précisant que la société MAMI demeurait responsable de tous les ordres de paiement. MAMI a donc formé opposition, mais American Express continuait à honorer les ordres de paiement. Après quelques mois, l'émetteur a demandé remboursement, mais la société MAMI l'a refusé. La cour d'appel de Versailles a condamné la société MAMI en se fondant sur les conditions générales du contrat d'où il résultait que, sauf en cas de vol ou de perte, la personne morale qui a sollicité l'établissement de la carte et son titulaire restaient solidairement responsable du règlement des dépenses effectuées avec la carte. La Cour de cassation casse l'arrêt en précisant que « sans rechercher si l'établissement émetteur de la carte avait, après avoir reçu opposition à son utilisation, mis en œuvre tous les moyens en sa disposition pour éviter que des retraits et ordres de paiement soient effectués, la cour d'appel n'a pas donné de base légale à sa décision ». Il ressort alors de l'arrêt que l'émetteur est obligé de réagir à la mise en opposition, bien qu'il soit persuadé que l'opposition n'est pas motivée par la perte ou le vol. La formule employée par la Cour de cassation rappelle fortement l'article 9, paragraphe 2 de la recommandation de la Commission européenne concernant les opérations effectuées au moyen d'instruments de paiement électronique.

227 Dans sa note sous l'arrêt précité de la cour d'appel d'Orléans, C. LUCAS de LEYSSAC approuve le principe selon lequel le banquier n'est pas juge du bien-fondé des oppositions. En se referant à l'analyse de D. MARTIN[149], il soutient que « dès lors que la régularité du mandat est en cause, il ne saurait être question d'ériger le mandataire en censeur de son mandant » et qu'alors l'émetteur qui reçoit une opposition « doit se contenter de l'enregistrer, et est tenu de ne pas débiter le compte de son client jusqu'à la

[147] CA Orléans, 2 févr. 1994, CRCAM Vosges c/ Mme Pierre, *D.* 1998, Jur., p. 37, note C. LUCAS de LEYSSAC.
[148] Cass. com., 20 oct. 1998, Sté Matériel Auxiliaire Marine et Industrie (MAMI) c/ Sté American Express Carte France, *JCP* éd. E 1999, p. 1101, note J. Devèze.
[149] D. MARTIN, « Analyse juridique du règlement par carte de payement », *D.* 1987, Chron., p. 52.

solution du litige »[150].

Mais C. LUCAS de LEYSSAC raisonne encore plus loin et justifie l'admissibilité de l'opposition au paiement pour une autre cause que la perte ou le vol de la carte. Il dénonce la confusion entre l'opposition au paiement par carte et l'opposition au paiement d'un chèque qui a mené certains auteurs aux conclusions que l'énumération légale concernant les oppositions au paiement par carte est limitative. L'opposition au paiement d'un chèque équivaut à la révocation d'un titre régulièrement émis, tant dis que l'opposition de l'article L. 132-2 du Code monétaire et financier est une mesure destinée à prévenir les risques liés à l'utilisation indue d'instrument permettant de donner un ordre de paiement. Alors, si l'opposition au paiement d'un chèque est réglementée strictement pour assurer la sécurité de la circulation du titre, il n'y a aucune raison logique de transposer ce régime à l'opposition au paiement par carte qui n'est pas un titre et ne circule pas[151].

228 Il est donc souhaitable d'admettre les oppositions chaque fois que l'ordre de paiement n'a pas été donné par la personne autorisée. C'est ce que le projet de loi relative à la sécurité quotidienne prévoit en matière des cartes de paiement. L'article 7 du projet de loi modifie l'article L. 132-2 du Code monétaire et financier et rend possible la mise en opposition en cas d'utilisation frauduleuse de la carte. Pour prévenir une interprétation restrictive de la formulation, l'Assemblée nationale a inséré parmi les cas où l'opposition est possible l'utilisation frauduleuse des « numéros » de la carte. Pour élargir le champ des hypothèses, le Sénat a à son tour adopté une rédaction différente autorisant l'opposition en cas d'utilisation frauduleuse des « données liées à son utilisation ».

229 La mise en opposition en cas d'ordre frauduleux donné sur Internet par l'envoi du numéro d'identification apparent de la carte devrait être finalement possible. Mais, nous devons préciser que cette opposition ne suit pas le régime de l'opposition telle que nous l'avons présenté pour les situations de perte ou de vol de la carte. Elle ne va pas conduire au partage des pertes dues à l'utilisation frauduleuse comme en cas de perte ou de vol. Le projet de loi l'exprime à l'article 7 *quater* en établissant que « la responsabilité du titulaire n'est pas engagée ». Les paiements seront annulés et les sommes remboursées au titulaire de la carte. Dans ce « régime allégé » de l'opposition seule subsiste l'obligation de l'émetteur de faire tout ce qui est raisonnablement en son pouvoir pour empêcher toute nouvelle utilisation de l'instrument de paiement électronique. L'émetteur sera alors contraint d'inscrire la carte dans le fichier des cartes en opposition. Tout le reste de la procédure d'opposition est supplanté par la procédure de remboursement que nous avons décrit précédemment.

230 La recommandation de la Commission européenne du 30 juillet 1997 instaure ce régime pour tous les instruments de paiement d'accès à distance utilisés dans certaines circonstances. Au paragraphe 3 de l'article 6, la recommandation prévoit : « La responsabilité du titulaire n'est pas engagée si l'instrument de paiement a été utilisé sans présentation physique ou sans identification électronique (de l'instrument même). »

Et la disposition continue : « La seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire. » Mais cette dernière phrase ne concerne plus le système de paiement vulnérable, elle nous conduit déjà à l'étude de la défense du titulaire contre les ordres de paiement frauduleux dans le système de paiement sécurisé.

---

[150] CA Orléans, 2 févr. 1994, CRCAM Vosges c/ Mme Pierre, *D.* 1998, Jur., p. 38, note C. LUCAS de LEYSSAC.

[151] J. DEVEZE, note sous Cass. com., 20 oct. 1998, précitée.

Section 2

Le système de paiement sécurisé

231 Par opposition au système de paiement vulnérable, nous entendons par système de paiement sécurisé celui qui dispose d'un procédé fiable d'identification. À l'heure actuelle, les solutions de paiement sur Internet utilisant un système de paiement sécurisé se font de plus en plus nombreuses. La signature électronique n'étant pas souvent utilisée, l'identification du titulaire passe la plupart du temps par la composition d'un code confidentiel.

Même un système de paiement sécurisé n'est pas irrésistible à la fraude. Ainsi, il se peut que le titulaire d'un moyen de paiement sécurisé découvre que son compte bancaire ou virtuel a été débité sans qu'il ait pu le supposer. Il est clair que le titulaire ne doit pas avoir à supporter les conséquences de la fraude même si le moyen de paiement est sécurisé[152].

Mais il est alors évident que le régime juridique applicable à la défense du titulaire contre les ordres frauduleux donnés dans un système de paiement sécurisé ne peut pas consister dans la présomption d'ordre frauduleux. Le problème de la charge de la preuve s'impose.

S'il paraît être accepté que la charge de la preuve ne doit pas reposer sur le titulaire (§ 1.), la situation du titulaire n'en est pourtant pas moins difficile (§ 2.).

§ 1. La charge de la preuve ne devant pas reposer sur le titulaire

232 La recommandation de la Commission européenne du 30 juillet 1997 contient au paragraphe 3 de l'article 6 une phrase irritant les émetteurs. En France, elle n'avait pas la chance d'être transposée dans le projet de loi relative à la sécurité quotidienne[153]. La disposition prévoit que « la seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire ». Dans le contexte de l'article 6, cela veut dire que l'utilisation d'un code confidentiel ne peut pas à elle seule prouver que l'ordre de paiement n'a pas été frauduleux et donc que le titulaire ne peut pas prétendre au remboursement. L'utilisation du code confidentiel ne doit pas établir la présomption de régularité de l'ordre de paiement.

La disposition est plus compréhensible si l'on y ajoute celle de l'article 7, paragraphe 2, e) d'après laquelle l'émetteur doit dans tout différend avec le titulaire, sans préjudice d'une preuve contraire produite par le titulaire, apporter la preuve que l'opération a été correctement enregistrée et comptabilisée et qu'elle n'a pas été affectée par un incident technique ou une autre défaillance.

233 D'après la recommandation, c'est alors l'émetteur qui, lorsqu'une opération est contestée par le titulaire, doit apporter la preuve de l'absence de dysfonctionnement du

---

[152] C'est ce que rappelle également la Communication de la Commission européenne « Prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces », COM (2001) 11, p. 8, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11fr.pdf .

[153] Selon le rapport d'information de M. Jean-Pierre BRARD du 11 juillet 2001, n° 3229, disponible sur www.assemblee-nationale.fr ,le Groupement des cartes bancaires a dénoncé les amendements qui devaient transposer ladite disposition « inappropriés, voir graves ».

système de paiement et doit accepter que le titulaire apporte la preuve contraire.

En droit français, en vertu de l'article 1315, alinéa 2 du Code civil, ce serait aussi à l'émetteur de démontrer l'absence d'irrégularité et par cela sa libération de l'obligation de restituer la somme. Mais la pratique a montré que les contrats passés entre l'émetteur de cartes et le titulaire contenaient souvent des clauses qui interdisaient au titulaire de contester l'ordre de paiement donné au moyen de la carte avec l'usage du code secret.

234 Ainsi, la Commission des clauses abusives française a recommandé[154], en relation avec les contrats porteurs des cartes de paiement, que soient éliminées des contrats les clauses conférant à l'usage de la carte avec un code confidentiel une valeur probante que le titulaire de la carte ne peut combattre.

235 Ces clauses ne se trouvent plus dans les contrats qui mettent à la disposition une carte de paiement. Or, la situation est différente pour d'autres systèmes de paiement. Nous avons découvert une clause qui pourrait être regardée comme abusive par exemple dans les conditions générales du portefeuille virtuel Odysseo[155], la solution de paiement française sur Internet. Dans ce document, il est prévu que le client est seul responsable de l'utilisation et la conservation du code confidentiel et qu'il assume notamment l'utilisation de son code confidentiel par une tierce personne. Une clause de portée identique se trouve dans la Convention BNP Net, l'application de banque par Internet de BNP Paribas. Cette convention stipule à l'article 14.1 qu'il est « expressément convenu que […] tout ordre précédé de la frappe du numéro d'abonné et du code secret est réputé émaner de l'abonné lui-même […] »[156].

236 Dans les situations où le contrat-cadre contient une telle clause, l'émetteur n'acceptera pas une demande d'annulation du paiement et de remboursement formée par le titulaire. Ce dernier devrait agir en justice pour que le juge déclare la clause abusive et la répute non écrite. Mais même si cet obstacle est franchi, ou si le contrat-cadre ne contient pas la clause problématique, la situation du titulaire reste dans la plupart des cas difficile.

§ 2. La situation pourtant difficile du titulaire

237 Si le titulaire forme opposition, celle-ci doit être acceptée dans toutes les circonstances, vu le principe que l'émetteur n'a pas à se faire juge de sa validité. Le titulaire d'un moyen de paiement dont il prétend qu'il a été utilisé frauduleusement, devrait donc être sûr de l'invalidation de son moyen de paiement. Mais si par exemple le code confidentiel est modifiable à tout moment à l'initiative du titulaire, ce qui est usuel lorsque le code confidentiel fonctionne comme un code d'accès au service[157], la mise en opposition n'est pas indispensable.

238 Pour le titulaire, c'est surtout la question du remboursement qui est importante. La restitution des fonds qui ont été transférés à la suite d'un ordre de paiement prétendu frauduleux par le titulaire est difficile à obtenir.

Si le contrat entre l'émetteur et le titulaire ne défend plus à ce dernier de contester

[154] La recommandation de la Commission des clauses abusives n° 94-02 relative aux contrats porteurs des cartes de paiement assorties ou non d'un crédit (BOCCRF 27 septembre 1994).
[155] www.odysseo.com .
[156] La convention est disponible sur www.bnpnet.bnp.fr/html/f_conv.htm .
[157] Voir la Convention BNP Net précitée, article 3. Mais la Convention permet également former opposition qui peut, de plus, être effectuée sans aucune justification. Pour cela, voir l'article 5.

l'ordre de paiement dans un système de paiement sécurisé, la preuve de l'absence de dysfonctionnement, que doit apporter l'émetteur, est souvent stipulée très formelle. Dans une telle situation, le titulaire du moyen de paiement sera contraint de fournir la preuve contraire ce qui mène au renversement de la charge de la preuve au préjudice du titulaire.

239 L'étude sur la conformité de la législation des États membres de l'Union européenne avec la recommandation du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique[158] a révélé que dans de nombreux pays, la question de la charge de la preuve n'est pas claire. Les contrats dans certains pays, parmi lesquels la France est citée, stipulent que les enregistrements internes de l'émetteur constituent la preuve de l'opération. Nous pouvons trouver cette clause à l'article 8 du contrat « Carte bancaire ». Elle devrait être changée dans la nouvelle rédaction du contrat, suite à la signature de la « Charte relative à la sécurité des cartes de paiement »[159] par les établissements émetteurs de cartes de paiement. Les contrats-cadres des diverses solutions françaises de paiement sur Internet comprennent des clauses allant dans le même sens.

240 Il est vrai qu'une clause sur la preuve est nécessaire, justement, par exemple, en droit français qui fait partie des ordres juridiques connaissant le régime de la preuve légale. La signature électronique étant dans la majorité des cas absente des ordres de paiement, les émetteurs doivent conclure avec les titulaires des moyens de paiement une convention relative à la preuve. Sinon, en vertu de l'article 1341 du Code civil, les émetteurs ne sauraient prouver les actes mixtes excédant 5 000 F.

Or, le problème posé par l'article 1341 du Code civil est celui de l'admissibilité de la preuve. Par contre, les clauses sus-visées n'établissent pas seulement l'admissibilité comme preuve des enregistrements électroniques internes. Elles opèrent aussi le renversement de la charge de la preuve, en employant la formule qui dit que les enregistrements justifient l'imputation des opérations au compte sur lequel fonctionne le moyen de paiement. Comme conclut l'étude de la transposition de la recommandation, en pratique, il paraît que l'émetteur apporte ses enregistrements internes comme preuve et le titulaire est contraint de démonter le dysfonctionnement du système ou la fraude.

241 Si le titulaire parvient pourtant à établir que l'ordre de paiement contesté est frauduleux et donc nul, il pourra espérer le remboursement. L'émetteur pourra encore tenter de démontrer la faute du titulaire qui a engendré la fraude. Si nous raisonnons par analogie à la réglementation prochaine concernant les cartes de paiement en France et la recommandation communautaire concernant tous les instruments de paiement d'accès à distance, il est possible de penser qu'une négligence du titulaire constituant une faute lourde pourrait exonérer l'émetteur de son obligation de remboursement.

242 Nous pouvons finalement remarquer que les chiffres alarmants du taux d'ordres de paiement frauduleux sur Internet ont fait réagir les législateurs. Ils ont concouru à la prévention contre les ordres de paiement frauduleux sur Internet, en instaurant la protection des données permettant d'ordonner le paiement sur Internet. De même, ils ont amélioré, ou tendent à le faire, les possibilités de défense de l'ayant droit contre les ordres de paiement frauduleux sur Internet.

---

[158] « Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment intruments and in particular the relationship between holder and issuer », Final Report, 20 mars 2001, p. 82, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.htm .

[159] La charte est disponible sur www.afb.fr/securitecarte.htm .

Conclusion

243 L'ordre de paiement sur Internet est un acte juridique. Il est régi par le droit contractuel. La liberté contractuelle et l'égalité des parties constituent les principes fondamentaux de ce droit.

La réalité ne répond pas toujours à ces principes. Les ordres de paiement s'insèrent dans le cadre contractuel bâti par les contrats d'adhésion. Le donneur d'ordre se trouve dans une position d'infériorité par rapport à l'émetteur du moyen de paiement.

Le législateur a pris l'habitude de rééquilibrer à l'aide des dispositions contraignantes les rapports de force entre les parties contractantes étant dans des positions différentes. Tout au début de notre étude, nous avons remarqué que le droit ne réagit qu' *a posteriori*. Le sort des relations qui jaillissent de l'ordre de paiement sur Internet en constitue un bel exemple.

Avec l'apparition du paiement sur Internet, des contrats entre les consommateurs et les émetteurs ont essayé d'apporter les réponses aux problèmes posés par Internet, à savoir les problèmes relatifs à l'identification et la sécurité sur Internet. Or, parce qu'il s'agit des contrats d'adhésion, les solutions apportées étaient souvent plus favorables aux émetteurs. Ainsi, en ce qui concerne les possibilités de défense de l'ayant droit contre les ordres de paiement frauduleux sur Internet, le législateur doit poser des limites à la liberté contractuelle qui était en pratique défavorable aux ayants droit.

244 Dans d'autres cas, le droit lui-même était la source des problèmes relatifs aux ordres de paiement sur Internet. Par la réglementation trop stricte de la cryptographie, il empêchait la mise en œuvre des procédés protégeant les données permettant d'ordonner le paiement sur Internet.

Les règles du droit de la preuve ont mérité également d'être adaptées à l'espace virtuel, ce qui a été fait par les textes sur les signatures électroniques.

En ce qui concerne la question de l'irrévocabilité de l'ordre de paiement sur Internet, les analyses économiques ont montré qu'il est quelquefois opportun d'atténuer le principe d'irrévocabilité posé par le droit.

245 En effectuant les comparaisons de divers ordres juridiques, nous avons découvert que les philosophies soutenant les systèmes juridiques américain et européen diffèrent largement.

Le droit américain est traditionnellement beaucoup plus bénévole vis-à-vis de la fraude et il compense ce laxisme par de larges mesures protectrices des consommateurs. Les commerçants acceptent ce système, vu la forte concurrence sur le marché américain.

L'Europe est encline à lutter beaucoup plus contre la fraude et, d'un autre côté, elle cherche à instaurer un subtil équilibre entre les intérêts des acteurs en jeu.

Bibliographie

Ouvrages :

L. BERNET-ROLLANDE, « Principes de technique bancaire », Dunod 1997.

T. BONNEAU, *Droit bancaire*, 4e éd., Montchrestien 2001

Vocabulaire juridique, sous la direction de G. CORNU, Association Henri Capitant, Quadrige/Presses Universitaires de France, 2000.

Lamy Droit du financement, Éditions Lamy 2001.

Lamy Droit de l'informatique et des Réseaux, Éditions Lamy 2001.

F. TERRÉ, P. SIMLER, Y. LEQUETTE, « Droit civil, Les obligations », 7e éd., Dalloz 1999.

Documents officiels :

Assemblée Nationale (France) :

Avis de M. Jean-Pierre BRARD, au nom de la commission des finances, n° 2992, du 18 avril 2001, disponible sur www.assemblee-nationale.fr .

Rapport d'information de M. Jean-Pierre BRARD du 11 juillet 2001, n° 3229, disponible sur www.assemblee-nationale.fr .

Rapport de M. Bruno LE ROUX, au nom de la commission des lois, n° 3177, du 26 juin 2001, disponible sur www.assamblee-nationale.fr .

Conseil d'État (France) :

Conseil d'État, « Internet et les réseaux numériques », disponible sur http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm .

Organes communautaires :

Communication de la Commission européenne « Commerce électronique et services financiers », COM (2001) 66 final du 7 février 2001, disponible sur http://europa.eu.int/comm/internal_market/fr/finances/general/ecomfaq.htm .

Communication de la Commission européenne « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cyber-criminalité », COM(2000) 890 final du 26 janvier 2001, disponible sur http://europa.eu.int .

Communication de la Commission européenne « Prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces », COM (2001) 11, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11fr.pdf .

« Payment card chargeback when paying over Internet », First Sub-group meeting of the PSTDG and PSULG held on 4 July 2000, document MARKT/173/2000, disponible sur http://europa.eu.int .

Proposition de décision-cadre du Conseil visant à combattre la fraude et la contrefaçon des moyens de paiement autres que les espèces, COM (1999) 438 final du 14 septembre 1999, disponible sur http://europa.eu.int .

« Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment intruments and in particular the relationship between holder and issuer », Final Report, 20 mars 2001, disponible sur http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.htm .

CNUDCI :

Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques, document A/CN.9/493, www.uncitral.org/fr-index.htm .

Conseil de l'Europe :

Projet final de la Convention sur la cyber-criminalité, disponible sur http://conventions.coe.int/Treaty/FR/cadreprojets.htm .

OCDE :

« Le recours du consommateur dans un marché international : les remboursements », OECD/GD(96)142, disponible sur www.oecd.org//dsti/sti/it/consumer/prod/f_96-142.pdf .

Articles et études:

H. ABELSON et L. LESSIG, « Digital Identity in Cyberspace », White Paper Submitted for 6.805/ Law of Cyberspace: Social Protocols, 10 December 1998.

Actualité bancaire, n° 449, du 3 mars 2001, p. 3, disponible sur www.afb.fr/ab.htm .

BAITAN, BERGER, MAIA, « Le protocole SSL (Secure Socket Layer) », 22 mai 1998, disponible sur www.esigge.ch/reche98/protoSSL/SSL.htm .

A. BENSOUSSAN, « Signature électronique et preuve : évolution ou révolution », *RJC* janvier 2001, n° spécial, Le droit des affaires du XXI^{e} siècle, p.43 s.

K. BÖHLE, « The Potential of Server-based Internet Payment Systems, An attempt to assess the future of Internet payments », Background Paper n° 3, *e*PSO, mars 2001, disponible sur http://epso.jrc.es/ .

P. BORIES, « Internet payant : nécessités et réalités », *JDNet*, le 29 juin 2001, http://solutions.journaldunet.com/0106/010629intro_dossier_payant.shtml/ .

P. BORIES, « Juin 2001, l'Odysseo de Blueline », *JDNet Solutions*, 5 juin 2001, http://solutions.journaldunet.com/0106/010605_blueline.shtml .

D. BOUNIE et L. VANINETTI, « E-payments : Which Systems in Europe for the Comming Years ? », *STAR Issue Report* n° 13, juin 2001, disponible sur www.databank.it/star/list_issue/g.html après l'inscription.

G. BRAIBANT, « Données personnelles et la société de l'information », rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998, disponible sur www.ladocfrancaise.gouv.fr .

P. BRUMFIELD FRY, « A PreliminaryAnalysis of Federal and State Electronic Commerce Laws », 2000, www.uetaonline.com/docs/pfry700.html .

J.-P. BUYLE, « Le paiement sur internet », *J.T.* 2001, p. 129. L'article est reproduit sur le site de *Droit et* nouvelles *technologies*, www.droit-technologie.org/fr/index.asp .

E. A. CAPRIOLI, « La loi du 13 mars 2000 », *RDBF* mai/juin 2000, Actualités, n° 106, p. 166.

E. A. CAPRIOLI, « Sécurité et confiance dans le commerce électronique, Signature numérique et autorité de certification », *JCP* éd. G 1998, I, 123, p. 583 s.

C. CHASSIGNEUX, « La protection des données personnelles en France », *Lex Electronica*, vol. 6, n° 2, hiver 2001, www.lex-electronica.org/articles/v6-2/chassigneux.htm .

S. DUSOLLIER et L. ROLIN-JACQUEMYNS, « Le défi du droit face au commerce électronique : les initiatives de l'Union Européenne », *Systèmes d'information et de management*, n° 1, Vol. 5, 2000, disponible sur www.droit.fundp.ac.be/crid/eclip/default.htm

R.-C. ÉCONOMIDES-APOSTOLIDIS, « La nature juridique des relations issues de l'utilisation d'une carte de crédit dans le droit des États membres dela C.E.E. », *RIDC* 1994, n° 4, p. 1023 s.

M. ESPAGNON, « L'ordre de paiement émis sur internet », *Rev. dr. bancaire* 1999, n° 71, p. 7 s.

M. ESPAGNON, « Le paiement d'une somme d'argent sur Internet : évolution ou révolution du droit des moyens de paiement ?, *JCP* éd. G 1999, I, 131, p. 787 s.

M. ESPAGNON, « Le paiement électronique en réseau "ouvert" – Internet : problématique juridique », *DIT* 1997/4, p. 6 s.

D. FELIX, « Paiement en ligne, un risque pour les sites marchands », *Les Echos*, 8 et 9 déc. 2000, p. 55.

P.-Y. GAUTIER et X. LINANT de BELLEFONDS, « De l'écrit électronique et des signatures qui s'y attachent », *JCP* éd. E 2000, p. 1273 s.

D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sou forme électronique », *J.T.* 2001, p. 114. L'article est reproduit sur le site de *Droit et nouvelles technologies*, www.droit-technologie.org/fr/index.asp .

D. GOBERT et A. SALAÜN, « La labellisation des sites web : Classification, stratégies et recommandations », *Droit et Nouvelles technologies*, dossier du 20 février 2000, disponible sur www.droit-technologie.org, .

F. GRUA, « Sur les ordres de paiement en général », *D.* 1996, 20e cahier, Chron., p. 172 s.

L. GRYNBAUM, « Loi du 13 mars 2000 : la consécration de l'écrit et de la preuve électroniques au prix de la chute de l'acte authentique », *Communication – Commerce Électronique*, avril 2000, Chron., p. 12 s.

T. HASSLER, « La signature électronique ou la nouvelle frontière probatoire », *RJC* 2000, p. 193 s.

J. HUET, « Aspects juridiques du télépaiement », *JCP éd. G* 1991, I, 3524, p. 287 s.

M. JASOR, « Forte progression de la fraude à la carte bancaire dans les paiements à distance », *Les Échos*, 24 et 25 novembre 2000, p. 1 et 36.

D. KAPLAN, « La France dans la société de l'information », mai 2001, disponible sur http://www.premier-ministre.gouv.fr/fr/p.cfm?ref=25274#1 .

S. LANSKOY, « La nature juridique de la monnaie électronique », *Bulletin de la Banque de France*, n° 70, octobre 1999, p. 45 s.

P. LECLERCQ, « Le nouveau droit civil et commercial de la preuve et le rôle du juge », *Communication – Commerce Électronique*, mai 2000, Chron., p. 9 s.

C. LUCAS de LEYSSAC et X. LACAZE, « Le paiement en ligne », *Communication – Commerce Électronique*, fév. 2001, Chron., p. 13 s.

D. MARTIN, « Analyse juridique du règlement par carte de payement », *D.* 1987, Chron., p. 51 s.

A. McCULLAGH, W. CAELLI, P. LITTLE, « Signature Stripping : A Digital Dilemma », *The Journal of Information, Law and Technology (JILT)*, http://elj.warwick.ac.uk/jilt/01-1/mccullagh.html .

Ph. NATAF et J. LIGHTBURN, « La loi portant adaptation du droit de la preuve aux technologies de l'information », *JCP* éd. E 2000, p. 836 s.

C. PAUL, « Du droit et des libertés sur l'Internet. La co-régulation, contribution française pour une régulation mondiale », Rapport remis au Premier ministre, mai 2000, disponible sur www.internet.gouv.fr/francais/textesref/pagsi2/lsi/rapportcpaul ou www.ladocfrancaise.gouv.fr .

R. PICHLER, « Finality of Credit Card Payments and Consumer Confidence – Different Approches in the United States and in Europe », *ePSO Newsletter*, n° 5, février 2001, disponible sur www.epso.jrc.es

R. PICHLER, « Trust and Reliance – Enforcement and Compliance : Enhancing Consumer Confidence in the Electronic Marketplace », thèse Standford University, mai 2000, disponible sur www.law.standford.edu/library/special/rufus.thesis.pdf .

A. SALAÜN, « Étude européenne : le points sur la position des 15 à l'égard des instruments de paiement électronique », disponible sur www.droit.fundp.ac.be/textes/etude%20paiements.pdf .

« SET Secure Electronic Transaction Specification, Book 1 : Business Description », disponible sur www.setco.org/download/set_bk1.pdf .

P. P. SINT, « E-money Solution from Austria: Paysafecard.com », *ePSO Newsletter*, n° 6, mars 2001, disponible sur www.epso.jrc.es .

Notes et observations :

T. corr. Paris, 25 février 2000, *D.* 2000, Jur., p. 219, obs. X. Delpech ; *RDBF*, mai/juin 2000, p. 165, obs. E. A. Caprioli.

CA Aix-en-Provence, 18 juin 1984, *D.* 1986, IR., p. 326, obs. M. Vasseur.

CA Orléans, 2 févr. 1994, CRCAM Vosges c/ Mme Pierre, *D.* 1998, Jur., p. 37, note C. LUCAS de LEYSSAC.

CA Paris, 12 mai 1995, *Rev. dr. bancaire*, nov/déc. 1995, n° 52, p. 217, obs. Crédot et Gérard.

CA Paris, 8e ch. A, 8 juin 1999, Mlle Marcilhacy c/ CIC, *D.* 2000, Somm., p. 337, obs. B. Thullier ; *Dalloz Affaires* 1999, p. 1287, obs. X. D. ; *RTD com*. 1999, p. 939, obs. M. Cabrillac.

Cass. com., 26 janvier 1983, *D.* 1983, IR 469, obs. M. Vasseur ; *RTD com*. 1984, p. 129, obs. M Cabrillac et B. Teyssié.

Cass. com., 20 oct. 1998, Sté Matériel Auxiliaire Marine et Industrie (MAMI) c/ Sté American Express Carte France, *JCP* éd. E 1999, p. 1101, note J. Devèze.

Index analytique

(Les chiffres renvoient aux numéros des paragraphes)

Table des matières