LES DOCUMENTS DE TRAVAIL DU SÉNAT

Série LÉGISLATION COMPARÉE

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

n° LC 125 **Octobre 2003**

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

Sommaire

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

La sécurité des transactions réalisées par carte bancaire est assurée à la fois par des dispositions juridiques et par des mesures techniques.

Ainsi, en France, plusieurs articles de la **loi n ° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ont introduit dans le code monétaire et financier de nouvelles dispositions destinées à garantir la sécurité des paiements faits par carte**.

En effet, cette loi charge expressément la Banque de France d'« *assurer la sécurité des moyens de paiement* » et institue l'Observatoire de la sécurité des cartes de paiement. De plus, elle élargit les cas où le titulaire d'une carte peut faire opposition, définit les responsabilités respectives du titulaire et de l'établissement émetteur en cas de perte, de vol ou d'utilisation frauduleuse d'une carte et facilite la sanction de tous les actes préparatoires à la fraude, en les érigeant en infraction spécifique.

Indépendamment de ce dispositif juridique, la généralisation de la carte à puce, le développement du cryptage des informations utilisées pour les paiements en ligne et l'introduction de programmes de recoupement dans les centres d'autorisation de transaction constituent autant de moyens techniques permettant d'améliorer la sécurité des transactions réalisées par carte.

La présente étude examine **les principales dispositions d'ordre juridique adoptées par plusieurs pays européens (Allemagne, Belgique, Danemark, Espagne et Royaume-Uni) pour garantir la sécurité des transactions réalisées par carte**.

Elle analyse donc les **mesures législatives et réglementaires** prises à cet effet en les classant en quatre catégories : les dispositions générales relatives aux établissements financiers, celles qui encadrent les relations entre ces établissements et les titulaires de cartes bancaires, celles qui définissent les conditions que chacune des transactions réalisées par carte bancaire doit remplir, et les mesures pénales prises pour lutter contre la fraude.

Elle analyse également les **mesures d'ordre déontologique mises en œuvre par les établissements financiers et par les autres professionnels** . En effet, si par exemple les codes de bonne conduite n'ont aucun caractère contraignant, ils peuvent constituer, notamment au Royaume-Uni, un élément important de la réglementation, incluant notamment des éléments qui relèvent de la loi dans d'autres pays.

La recherche de la sécurité maximale constitue une préoccupation commune à tous les pays étudiés, mais les moyens mis en œuvre pour y parvenir varient beaucoup.

L'analyse révèle en effet que la transposition de la directive 97/7 du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance (document n° 1) et la prise en compte de la recommandation de la Commission européenne 97/489 du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique (document n° 2) ont entraîné une **relative uniformisation des règles de responsabilité des titulaires de cartes bancaires, ainsi que l'introduction dans les différents droits nationaux d'un délai de rétractation**, qui vise en particulier les achats réglés par carte bancaire.

En revanche**, les autres dispositions** adoptées pour garantir la sécurité des transactions réalisées par carte bancaire **diffèrent, tant par leur nature,** strictement juridique (lois et règlements) ou d'ordre plutôt déontologique (codes de bonne conduite des établissements financiers, labellisation des sites Internet garantissant la sécurité des paiements), **que par leur contenu** (amélioration de l'information des titulaires de cartes, création d'infractions pénales spécifiques…).

1) L'uniformisation entraînée par la transposition de la directive 97/7 et par la prise en compte de la recommandation 97/489

a) Les règles de responsabilité

Tous les pays sous revue ont adopté des règles de responsabilité qui protègent les titulaires de cartes bancaires et donc les mettent en sécurité : **en règle générale, l'utilisation frauduleuse de la carte bancaire n'a de**

conséquences pour les titulaires que s'ils ont fait preuve de négligence, par exemple en notant leur numéro de code confidentiel à proximité de la carte. Dans les autres cas, leur responsabilité n'est engagée que jusqu'à un certain plafond, qui varie de 50 à 150 €.

b) Le délai de rétractation

La transposition de la directive 97/7 a entraîné l'introduction d'un délai de rétractation en cas d'achat à distance. Fixé par la directive à sept jours, il est plus élevé dans deux des cinq pays étudiés, l'Allemagne et le Danemark, qui l'ont porté à quatorze jours. Si cette mesure ne vise pas spécifiquement la carte bancaire, elle est cependant importante pour développer la confiance des consommateurs, dans la mesure où la carte bancaire constitue un moyen commode de régler les achats effectués à distance.

2) L'extrême diversité des autres mesures

a) Des mesures de nature diverse

L'Allemagne, la Belgique et le Danemark s'appuient surtout sur des mesures législatives, à la différence de l'Espagne et du Royaume-Uni, qui insistent sur les « bonnes pratiques » des établissements financiers.

De plus, si **la Belgique et le Danemark ont récemment adopté des lois sur les moyens de paiement électronique**, qui s'appliquent en particulier aux transactions réalisées par carte bancaire, ce n'est pas le cas de l'Allemagne, où des dispositions très générales, telles celles du droit des contrats, sont considérées comme suffisantes.

Au Royaume-Uni, les banques adhèrent à un code de bonne conduite national, qui comprend des mesures visant à garantir la sécurité de la carte bancaire. En revanche, en Espagne, les établissements financiers se réfèrent au code de bonne conduite du secteur bancaire européen 14 novembre 1990 relatif aux systèmes de paiement par carte, ainsi qu'à la recommandation concernant les opérations effectuées au moyen de paiement électronique émise en 1997 par la Commission européenne.

b) Des mesures de contenu divers

L'exemple du Danemark et du Royaume-Uni, qui ont retenu des approches opposées, illustre cette diversité.

Le premier fait reposer l'essentiel de son dispositif de lutte contre la fraude aux cartes bancaires sur la prévention. L'information des détenteurs de cartes bancaires est très développée et l'*ombudsman* des consommateurs veille

à ce que les établissements financiers respectent les obligations que la loi leur impose, notamment en matière d'information des clients et de sécurité des procédures de paiement.

En revanche, **le Royaume-Uni**, où la fraude par copie de la piste magnétique des cartes bancaires constitue un réel fléau, **concentre une partie de ses efforts sur la lutte contre la criminalité informatique**. Ainsi, une force de police spécialisée dans la lutte contre les infractions commises grâce à Internet a été créée en 2000. Elle est notamment compétente pour les fraudes à la carte bancaire. En 2002, l'APACS, association qui regroupe la plupart des établissements financiers, a contribué, en collaboration avec le ministère de l'Intérieur, à la création d'un corps de police spécialisé dans la lutte contre la fraude aux moyens de paiement. Cette unité, financée à hauteur de 75 % par l'APACS, rassemble des officiers de police et des experts bancaires.

* *

*

Dans tous les pays étudiés, les résultats obtenus en France grâce à la technologie de la puce sont vantés. Ces remarques convergentes permettent de conclure que, **à l'intérieur d'un cadre juridique visant à garantir la sécurité maximale des transactions réalisées par carte bancaire, c'est aux établissements financiers qu'il appartient de prendre les mesures techniques nécessaires, notamment préventives**. C'est d'ailleurs ce que font les principaux réseaux de cartes bancaires avec l'introduction progressive de la carte à puce dans tous les pays de l'Union européenne d'ici le 1er janvier 2005.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

ALLEMAGNE

Il existe peu de dispositions législatives et réglementaires destinées spécifiquement à garantir la sécurité des transactions réalisées par carte bancaire. La plupart des règles applicables sont des **règles générales**, qui découlent notamment du droit des contrats, car elles sont considérées comme suffisamment souples pour couvrir les cas particuliers, y compris celui des relations entre, d'une part, les titulaires de cartes bancaires et, d'autre part, les commerçants ou les établissements financiers.

Cependant, avec l'entrée en vigueur le 1er juillet 2000 de la loi sur les **achats à distance,** adoptée pour transposer la directive 97/7, plusieurs mesures visant particulièrement la sécurité de la carte bancaire ont été introduites. La loi sur les achats à distance a été formellement abrogée le 31 décembre 2001, car ses dispositions ont alors été intégrées au code civil.

I. LES DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES

1) Le cadre général

Les pénalités appliquées aux établissements financiers qui ne respectent pas les dispositions de la **loi bancaire** sont considérées comme suffisamment dissuasives pour garantir, de façon indirecte, la sécurité des transactions réalisées par carte bancaire.

2) Les relations entre les établissements financiers et les titulaires de cartes bancaires

Elles sont définies dans les « conditions générales d'affaires » du secteur bancaire. Dans un certain nombre de secteurs, et en particulier celui de la consommation, les conditions générales d'affaires évitent l'élaboration de contrats individuels. Ces conditions générales doivent respecter les prescriptions du code civil, notamment en matière de responsabilité.

a) La limitation de la responsabilité des titulaires de cartes bancaires

L'article 676h du code civil, qui résulte de la codification de la loi sur les achats à distance, dispose que la banque ne peut exiger le paiement des dépenses réglées à l'aide d'une carte bancaire que si la carte n'a pas été utilisée de façon frauduleuse.

Cette disposition exclut donc toute mise en jeu de la responsabilité du titulaire en cas d'utilisation frauduleuse de sa carte, que le code confidentiel ait ou non été utilisé, à moins que la négligence du titulaire ne soit à l'origine de la fraude.

Les plafonds de responsabilité sont déterminés dans les conditions générales des banques. En règle générale, en cas de vol ou de perte dûment déclaré à la banque, le titulaire est responsable dans la limite de 50 €, tandis que, en cas de négligence, il est responsable à hauteur de 100 % ou de 90 % selon que la négligence est ou non qualifiée de grossière. Communiquer son code confidentiel à un tiers ou le noter sur la carte bancaire, ou à proximité immédiate, constituent des exemples de négligence grossière.

Une décision rendue en avril 2002 par la Cour fédérale suprême fait porter sur les établissements financiers, et non pas sur les commerçants comme auparavant, la responsabilité en cas d'utilisation frauduleuse des seules données d'une carte, c'est-à-dire lorsque la carte elle-même n'est pas présentée.

b) La mise en garde des titulaires de cartes bancaires

Les conditions générales des banques énoncent toutes les précautions que les titulaires de cartes bancaires doivent respecter pour préserver la sécurité des transactions, ainsi que les démarches à effectuer en cas de perte, de vol ou d'utilisation frauduleuse.

Le code civil précise que les conditions générales n'engagent les parties que si elles ne se présentent pas sous une forme « inhabituelle » et si leur interprétation n'est pas équivoque.

3) Les transactions individuelles

Le délai de rétractation

Les articles 355 et 356 du code civil, qui résultent de la codification de la loi sur les achats à distance, offrent aux consommateurs un délai de rétractation de **quatorze jours** et la possibilité d'obtenir le remboursement de leurs achats. Ces dispositions visent en particulier les achats réglés par carte bancaire.

4) Les mesures pénales

a) La falsification des cartes bancaires

D'après l'article 152a du **code pénal**, **la falsification de cartes bancaires constitue une infraction spécifique**.

Le fait d'utiliser des fausses cartes, d'en détenir ou d'en procurer à autrui tombe sous le coup du même article, qui prévoit une peine de prison dont la durée est comprise entre un et dix ans.

Lorsque l'infraction est commise par un réseau, la peine minimale est de deux ans de prison.

b) L'utilisation abusive des cartes bancaires par les titulaires

Elle constitue également, aux termes de l'article 266b du code pénal, une infraction spécifique, punissable d'une amende ou d'une peine de prison dont la durée maximale est de trois ans.

L'infraction définie par l'article 266b du code pénal consiste, par l'utilisation de sa propre carte, à créer un préjudice à l'émetteur de la carte. Elle vise les retraits d'argent liquide depuis des distributeurs n'appartenant pas au même réseau que celui de la banque qui a émis la carte.

Les autres utilisations abusives des cartes bancaires par les titulaires tombent sous le coup de l'article 263a du code pénal, relatif à la fraude informatique. Ils sont punissables d'une amende ou d'une peine de prison d'au plus cinq ans.

II. LES AUTRES MESURES

1) Les mesures prises par le secteur bancaire

L'utilisation du code à trois chiffres figurant au verso de la carte pour les achats à distance

Depuis avril 2001, les consommateurs ont l'obligation de fournir aux commerçants **le numéro à trois chiffres qui figure au verso leur carte** lorsqu'ils règlent un achat en utilisant celle-ci et qu'ils passent leur commande par téléphone, par courrier ou par Internet.

2) Les mesures prises par les commerçants

La multiplication des vérifications

Les commerçants, préoccupés par l'importance de la fraude, dont le coût pour l'économie allemande est estimé à environ 75 millions d'euros, parmi lesquels 46 imputables aux seules opérations réalisées en Allemagne, multiplient les contrôles : certains exigent que le client présente une pièce d'identité, d'autres qu'il compose son code secret même s'il a signé une facturette (et inversement).

3) Les mesures prises par la police

Le dispositif d'alerte des commerçants

Dans plusieurs *Länder* (en particulier ceux de Brandebourg, de Berlin, de Brême et de Saxe), la police utilise la messagerie électronique pour communiquer aux commerçants et aux établissements financiers les données relatives aux cartes volées, et ainsi empêcher la réalisation de transactions frauduleuses. Ce dispositif, **Kuno** (*Kriminalitätsbekämpfung im unbaren Zahlungsverkehr durch Nutzung nichtpolizeilicher Organisationsstrukturen*, c'est-à-dire lutte contre la criminalité relative aux transferts électroniques de fonds par l'emploi de structures non policières), a été imaginé par un commissaire de la ville de Dresde en août 2001 puis adopté par plusieurs *Länder*.

Kuno est considéré comme un moyen de lutte efficace lorsque la fraude repose sur l'utilisation de cartes à piste magnétique, car les lecteurs de cartes des commerçants ne sont pas reliés aux systèmes informatiques des banques, ce qui permet à une carte volée de continuer à être acceptée par les commerçants.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

BELGIQUE

La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds (document n° 3) s'applique notamment aux transactions réalisées par carte. Elle se fixe comme objectif de « *parvenir à une confiance totale des utilisateurs et d'assurer un degré élevé de protection des titulaires d'instruments de paiement dans l'utilisation des moyens de paiement électroniques* ». Cette loi comporte donc plusieurs dispositions sur la sécurité des transactions réalisées au moyen de cartes bancaires.

Il en va de même de la **loi du 14 juillet 1991** sur les pratiques du commerce et sur l'information et la protection du consommateur, depuis qu'elle a été modifiée par la loi du 25 mai 1999, laquelle transpose la directive 97/7 relative aux contrats à distance.

Par ailleurs, la **loi du 28 novembre 2000 relative à la criminalité informatique** a introduit dans le code pénal de nouvelles infractions, dont certaines se rapportent aux cartes bancaires.

I. LES DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES

1) Le cadre général

Aucune mesure générale ne vise spécifiquement la sécurité des cartes bancaires.

2) Les relations entre les établissements financiers et les titulaires de cartes bancaires

Elles sont essentiellement définies par la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, qui, de façon générale, sanctionne d'une amende comprise entre 500 € et 200 000 € les infractions aux règles qu'elle édicte, lorsque la « *mauvaise foi* » de l'auteur est établie.

a) La mise en garde des détenteurs de cartes bancaires

Préalablement à la conclusion d'un contrat relatif à la mise à disposition d'une carte bancaire, l'établissement financier émetteur de la carte doit communiquer à l'utilisateur les **conditions contractuelles d'utilisation**. Celles-ci « *sont présentées de manière claire et non équivoque, par écrit ou sur un support durable à la disposition du titulaire et auquel il a accès* ». D'après l'exposé des motifs du projet de loi, par « support durable », il faut entendre un support papier, une disquette, un CD-ROM, voire un autre dispositif permettant la transmission d'un message électronique.

Les conditions contractuelles comprennent les obligations et responsabilités respectives de l'émetteur de la carte et du titulaire, notamment les règles de prudence que le titulaire doit observer et les démarches qu'il doit effectuer en cas de perte, de vol ou d'utilisation frauduleuse.

En cas de non-respect de ces dispositions, l'émetteur est civilement responsable de toutes les conséquences résultant de l'utilisation frauduleuse de la carte bancaire, à moins que la fraude ne soit le fait du titulaire lui-même.

La loi oblige également les établissements financiers émetteurs de cartes bancaires à fournir « *périodiquement* » aux titulaires des «*conseils de prudence destinés à éviter tout usage abusif de* [la carte bancaire] *et des moyens qui en permettent l'utilisation* ».

b) L'obligation pour les établissements financiers émetteurs de cartes de garantir la confidentialité des codes secrets

L'émetteur (ou l'entreprise qu'il a désignée pour distribuer les cartes bancaires) a l'obligation de prendre toutes les mesures pour garantir la confidentialité du code secret du titulaire.

Cette disposition vise à rendre l'émetteur responsable entre le moment de l'envoi au titulaire de la carte et du code confidentiel et celui de sa réception.

c) La limitation de la responsabilité des détenteurs de cartes bancaires

En cas d'utilisation frauduleuse de la carte bancaire, la responsabilité du titulaire ne peut être engagée que dans deux cas : si l'instrument de paiement a été présenté physiquement ou, en cas d'utilisation à distance, s'il y a eu identification électronique, par exemple par insertion de la carte dans un terminal de paiement permettant de vérifier que la carte est authentique.

A contrario, en cas de paiement à distance réalisé par simple communication du numéro apparent de la carte et de sa date d'expiration sans identification électronique, la responsabilité du titulaire n'est pas engagée.

En cas de vol ou de perte, si le titulaire ne signale pas immédiatement à l'émetteur qu'il n'est plus en possession de sa carte, il est responsable à hauteur de 150 € jusqu'au moment de la notification des faits.

Toutefois, s'il a commis une négligence grave, par exemple en laissant son code confidentiel à proximité de sa carte, ou s'il a agi frauduleusement, ce plafond ne s'applique pas et le titulaire est responsable sans limites.

Aux termes de la loi, l'utilisation frauduleuse du titulaire peut notamment être constituée par le fait :

– de donner sa carte ainsi que son code confidentiel à un tiers et d'adresser ensuite une déclaration de perte ou de vol à l'établissement émetteur ;

– d'utiliser soi-même la carte après en avoir notifié le vol ou la perte à l'émetteur.

d) La fourniture aux titulaires de cartes bancaires d'informations relatives aux opérations réalisées

L'émetteur doit fournir périodiquement au titulaire des informations concernant les opérations effectuées au moyen de la carte bancaire. La périodicité est laissée à l'appréciation de l'émetteur, mais elle doit permettre au titulaire de suivre l'état de ses dépenses.

Ces informations doivent comprendre un certain nombre d'éléments définis par l'article 5 de la loi (date, montant, date de valeur, nom et adresse du bénéficiaire, commissions, frais…).

Les relevés des opérations effectuées au moyen d'un instrument de transfert électronique de fonds doivent être conservés pendant cinq ans par l'émetteur.

3) Les transactions individuelles

a) Le délai de rétractation

En règle générale, les signataires des **contrats à distance** bénéficient d'un **droit de renonciation** de **sept jours ouvrables**. Lorsque l'acheteur exerce son droit de renonciation, seuls les frais de renvoi peuvent être mis à sa charge.

b) La charge de la preuve pesant sur les établissements financiers

L'article 6 de la loi du 17 juillet 2002 impose à l'établissement financier émetteur de la carte d'apporter la preuve que toutes les opérations ont été correctement enregistrées et comptabilisées et n'ont pas été affectées par un incident technique ou par une défaillance. Le titulaire a la possibilité de contester les opérations dans les trois mois après la communication des informations concernant ces dernières.

4) Les mesures pénales

La loi du 26 novembre 2000 relative à la criminalité informatique a créé deux nouvelles infractions :

– **le faux en informatique**, qui fait l'objet du nouvel article 210 bis du code pénal, consiste notamment en la falsification ou la contrefaçon de cartes bancaires ;

– **la fraude informatique**, introduite par le nouvel article 504 quater du code pénal, vise par exemple l'utilisation d'une carte bancaire volée pour retirer de l'argent dans un distributeur automatique.

Les sanctions encourues pour ces infractions sont un emprisonnement de six mois à cinq ans et/ou une amende comprise entre 130 € et 500 000 €. La tentative est punie des mêmes peines que l'infraction elle-même.

II. LES AUTRES MESURES

1) Les mesures prises par le secteur bancaire

L'Association des banques belges a rédigé un **code de bonne conduite** définissant les règles que les banques doivent respecter dans leurs relations avec leurs clients.

La sécurité et la fiabilité des services bancaires, qui constituent l'un des sept principes de base définis par ce code, résultent, d'après ce document, de la qualité technique des systèmes utilisés et de leur utilisation attentive par les clients. Le code de bonne conduite reprend en effet quelques conseils de base à l'attention des clients concernant l'utilisation de la carte bancaire, la confidentialité du code secret et les formalités à effectuer en cas de perte ou de vol de la carte.

Par ailleurs, l'Association des Banques belges a édité plusieurs documents contenant des **conseils de sécurité à l'attention des titulaires** de cartes bancaires. Il leur est notamment recommandé de conserver les tickets de retrait et de paiement, de vérifier les relevés de compte dès qu'ils les reçoivent, et de demander aux commerçants qu'ils s'assurent de la concordance entre les données de la carte bancaire et celles de la carte d'identité ainsi que de la conformité de la signature apposée sur la facturette avec celle figurant au dos de la carte bancaire.

2) Les mesures prises par les autres professionnels

a) Le code de bonne conduite de la Fédération des entreprises de Belgique

En tant qu'organisation interprofessionnelle représentative de l'ensemble des secteurs d'activité, la Fédération des entreprises de Belgique a élaboré un code de bonne conduite applicable en matière de commerce électronique, qui régit à la fois les relations entre entreprises et les relations entre entreprises et consommateurs.

Les entreprises signataires s'engagent à assurer « *la fiabilité et la sécurité des transactions* ».

b) Le code de bonne conduite relatif au commerce électronique élaboré par la Fédération des chambres de commerce et d'industrie de Belgique et par Test-Achats

Ce code résulte d'une initiative de diverses organisations de consommateurs européennes, parmi lesquelles Test-Achats. Il bénéficie du soutien de la Commission européenne et du ministère belge de l'Économie. Les entreprises adhérant à ce code se voient attribuer un **label** qui garantit notamment la sécurité des paiements.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

DANEMARK

La loi du 31 mai 2000 sur « *certains moyens de paiement* » (document n° 4) est entrée en vigueur le 1er juillet 2000. Elle a abrogé la loi de 1994 sur les cartes de paiement, qui avait été amendée à plusieurs reprises depuis son entrée en vigueur.

La loi du 31 mai 2000 s'applique non seulement aux transactions réglées par carte, mais aussi à celles qui sont réalisées à l'aide de codes ou d'autres moyens personnels d'identification. Elle repose sur les mêmes principes que la loi précédente et se fixe pour objectif « *de garantir que les moyens de paiement qui entrent dans son champ d'application sont sûrs et fonctionnent bien* ». Elle comporte donc plusieurs dispositions visant à garantir la sécurité des opérations effectuées à l'aide d'une carte bancaire.

La loi du 23 décembre 1987 sur certains contrats de vente, modifiée plusieurs fois depuis son adoption, notamment pour transposer la directive 97/7, comporte également des mesures de sécurisation des transactions réglées par carte bancaire.

Par ailleurs, les professionnels, et notamment les établissements financiers, ont pris eux-mêmes des dispositions destinées à améliorer la sécurité des transactions réalisées par carte bancaire.

I. LES DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES

Les dispositions analysées ci-dessous figurent, d'une part, dans la loi du 31 mai 2000 et, d'autre part, dans celle du 23 décembre 1987.

1) Le cadre général

a) L'enregistrement préalable de tous les établissements financiers émetteurs de cartes bancaires auprès de l'ombudsman des consommateurs

Tous les établissements émetteurs de moyens de paiement, et donc **tous les émetteurs de cartes bancaires, ont l'obligation d'effectuer une déclaration préalable de leur activité auprès de l'*ombudsman* des consommateurs.**

La déclaration comporte le nom, l'adresse et la raison sociale. Elle précise également **les informations données aux consommateurs qui souscrivent un contrat pour la mise à disposition d'une carte bancaire**.

Le défaut de déclaration est sanctionné d'une amende.

b) Le contrôle de l'ombudsman des consommateurs

L'*ombudsman* des consommateurs veille à la bonne exécution de la loi du 31 mai 2000. Il doit en particulier s'assurer que les procédures mises en place assurent la sécurité de l'ensemble des moyens de paiement et que les pratiques des professionnels prennent en compte les intérêts des consommateurs *(1).*

Pour exercer sa mission, l'*ombudsman* peut exiger tous les renseignements qu'il juge utile. Il peut s'entourer d'experts. S'il estime qu'une pratique ne respecte pas le cadre législatif et s'il ne parvient pas à un accord avec le professionnel concerné, il peut lui adresser une **injonction**. Si celle-ci n'est pas suivie d'effet, l'*ombudsman* peut entamer une procédure judiciaire.

Les décisions que l'*ombudsman* prend dans le cadre de la loi du 31 mai 2000 ne sont pas susceptibles de recours devant une autre autorité administrative.

2) Les relations entre les établissements financiers et les titulaires de cartes bancaires

a) La limitation de la responsabilité des titulaires de cartes bancaires

En cas de fraude, le principe consiste à attribuer la responsabilité aux émetteurs, sauf si le code confidentiel est utilisé. Dans cette hypothèse, le

(1) Le contrôle de l'ombudsman des consommateurs est totalement indépendant de celui qui est pratiqué par l'autorité de surveillance des activités financières.

titulaire voit donc sa responsabilité engagée, même s'il n'a pas communiqué le code à un tiers.

Lorsqu'il n'a pas communiqué le code confidentiel à un tiers, la responsabilité du titulaire est généralement engagée de façon limitée : **jusqu'à 1 200 ou 8 000 couronnes** (c'est-à-dire 160 ou 1 080 €) selon les circonstances *(2)* :

> – 1 200 couronnes, lorsque le code confidentiel du titulaire de la carte a été utilisé ;
>
> – 8 000 couronnes, lorsque le code confidentiel du titulaire de la carte a été utilisé et que ce dernier a, de surcroît, fait preuve de négligence (en omettant d'indiquer à sa banque le vol de sa carte, en communiquant son code ou en commettant une autre négligence grossière, permettant ainsi la fraude). C'est à la banque qu'il appartient de prouver la négligence du titulaire pour que la limite de responsabilité soit portée à 8 000 couronnes.

La responsabilité du titulaire est toutefois engagée sans limite lorsqu'il a communiqué son code confidentiel à la personne qui a utilisé frauduleusement la carte bancaire et que la fraude a eu lieu dans des circonstances où il aurait dû se rendre compte qu'il courait un risque.

En cas **d'utilisation frauduleuse** de la carte bancaire **sans utilisation du code confidentiel** (par exemple, lorsque la transaction a été réalisée uniquement à l'aide du numéro de la carte et de la date de fin de validité), la responsabilité du titulaire de la carte n'est engagée que si la signature de ce dernier a été contrefaite et si une négligence grossière du titulaire a permis la fraude. La responsabilité du titulaire n'est engagée que si l'émetteur prouve la négligence du titulaire. En outre, elle ne peut pas l'être pour un montant supérieur à 8000 couronnes.

Les plafonds de responsabilité s'appliquent à l'ensemble des opérations frauduleuses effectuées par un tiers, et non à chaque transaction.

b) La mise en garde des titulaires de cartes bancaires

Les émetteurs de carte bancaire doivent **fournir aux utilisateurs des renseignements** exprimés « *dans un langage simple et compréhensible* », **sur l'utilisation sûre et appropriée des cartes**, la loi laissant les émetteurs libres de déterminer la nature précise de ces informations ainsi que la voie par laquelle elles sont communiquées.

Ils doivent également attirer l'attention des utilisateurs sur les démarches à effectuer lorsque leur carte bancaire a été utilisée frauduleusement et sur l'engagement de leur responsabilité en pareil cas.

(2) Comme ces dispositions reprennent en grande partie celles de la loi précédente, qui prévoyait les mêmes plafonds de responsabilité, on peut estimer que, dans la majorité des cas, la limite de responsabilité sera de 1 200 couronnes.

Le non-respect de cette obligation est sanctionné d'une amende.

3) Les transactions individuelles

a) La fourniture aux titulaires de cartes bancaires d'un reçu à l'occasion de chaque transaction

Alors que la loi précédente faisait de la fourniture d'un reçu une obligation qui ne souffrait aucune exception, **la loi de 2000 assouplit les contraintes pesant sur les fournisseurs** : elle dispose que le consommateur a droit à un reçu à l'occasion de chaque transaction, à moins qu'il ne dispose d'un autre moyen le renseignant sur le montant et la date de l'opération.

D'après les travaux préparatoires à la loi de 2000, le reçu doit être un document écrit lorsque la carte bancaire est utilisée de façon « classique », dans un magasin par exemple. En revanche, dans le cas d'achats à distance par exemple, un reçu adressé par courrier électronique peut suffire.

b) Le délai de rétractation

En règle générale, les achats sont fermes et définitifs. Cependant, la législation sur les consommateurs prévoit plusieurs exceptions à ce précepte. La principale, qui concerne les **achats par correspondance**, vise notamment les paiements réalisés par carte bancaire.

L'acheteur dispose d'un **délai de rétractation de quatorze jours**. Dans la mesure où il renvoie la marchandise dans l'état où il l'a reçue, il n'encourt aucuns frais, sauf les frais de transport. Il peut donc obtenir le remboursement intégral de son achat.

c) Le remboursement de tout débit injustifié

La loi de 1994 comportait un alinéa obligeant les établissements financiers à prouver que les débits effectués sur les comptes des clients ne résultaient pas d'erreurs d'ordre technique ou informatique. De cette disposition, l'*ombudsman* des consommateurs a tiré la conclusion que tous les débits devaient être prouvés par les établissements financiers et que, par conséquent, les consommateurs pouvaient obtenir le remboursement de tout débit injustifié : que celui-ci dépasse le montant de l'achat prévu, ou que la marchandise ou la prestation n'ait pas été fournie par exemple.

La loi de mai 2000 reprend exactement la même disposition que la loi précédente. Elle donne donc lieu à la même interprétation.

4) Les mesures pénales

Actuellement **l'utilisation frauduleuse de cartes bancaires ne fait pas l'objet de dispositions pénales spécifiques** et les articles du code pénal relatifs à la fausse monnaie ne leur sont pas applicables. Ces infractions tombent donc sous le coup des articles du code pénal relatifs à l'**escroquerie** et à l'escroquerie informatique. Cependant, préoccupé par le développement de la délinquance d'ordre informatique, le ministère de la Justice a, en octobre 1997, désigné un groupe de travail qu'il a chargé de réfléchir aux évolutions législatives souhaitables.

À la fin de l'année 2002, le groupe de travail a rendu son rapport et, s'appuyant sur ses recommandations, le ministère de le la Justice a préparé un **avant-projet de loi**. Ce dernier prévoit notamment une modification du chapitre consacré à la fausse monnaie, dont l'intitulé deviendrait « Infractions contre les moyens de paiement » et qui comprendrait un article punissant explicitement la fabrication, la diffusion et l'acquisition de moyens de paiement électroniques, parmi lesquels les cartes bancaires.

II. LES AUTRES MESURES

1) Les mesures prises par le secteur bancaire

a) L'utilisation du code à trois chiffres figurant au verso de la carte pour les achats à distance

Depuis **avril 2002**, PBS (qui est en quelque sorte l'équivalent du GIE français Carte bancaire) exige que les consommateurs indiquent aux commerçants, outre le numéro et la date de fin de validité de leur carte bancaire, **le numéro à trois chiffres qui figure au verso** de leur carte lorsqu'ils règlent un achat au moyen de celle-ci et qu'ils passent leur commande par téléphone, par correspondance ou par Internet.

Les commerçants ont ensuite l'obligation de transmettre ce code à PBS, qui vérifie la cohérence entre les trois éléments fournis.

Le défaut de fourniture de ce code entraîne le rejet de la transaction.

b) La modernisation des cartes bancaires

Une modification de la loi de mai 2000, adoptée le 4 juin 2003 et qui entrera en vigueur le 1er janvier 2005, va permettre aux professionnels de moderniser le système de paiement par carte.

En effet, dans sa version initiale, l'article 14 de la loi interdisait aux établissements financiers de faire payer aux commerçants des droits *(3)* lorsque les clients utilisaient leur carte de façon « classique », c'est-à-dire lorsque la transaction se réalisait en présence du client et du commerçant. Le prélèvement d'un droit était en revanche possible si la carte était utilisée pour régler un achat effectué à distance.

La modification adoptée permet aux établissements financiers de prélever sur les commerçants un droit sur toutes les opérations réalisées sur place à l'aide d'une **carte à puce**. Le montant de ce droit varie en fonction de plusieurs éléments (âge du titulaire, carte valable ou non à l'étranger…). En règle générale, il s'élève à 0,50 couronnes (soit un peu moins de 0,07 €) par transaction. En revanche, si les paiements sont effectués à l'aide d'une carte dotée seulement d'une piste magnétique, aucun droit ne sera exigible.

Les commerçants pourront répercuter cette somme sur les clients, dans la limite du droit qu'ils paient eux-mêmes.

Ces règles, valables jusqu'au 31 décembre 2009, seront remplacées par de nouvelles dispositions à partir du 1er janvier 2010.

2) Les directives de l'ombudsman des consommateurs

Élaborées conformément à la loi de 1994 sur les cartes de paiement, elles ont été abrogées en mars 2002. Toutefois, elles continuent à être suivies par les professionnels, en attendant que de nouvelles directives soient rédigées.

Les directives de l'*ombudsman* des consommateurs résultent de la collaboration entre les représentants des établissements financiers, des consommateurs et des commerçants.

Elles ne valent que pour les **achats effectués à distance** et cherchent à offrir aux consommateurs la protection maximale contre toute utilisation frauduleuse de leur carte. L'objectif principal des directives consiste à obliger les émetteurs des cartes et les bénéficiaires des paiements à suivre des procédures assurant aux titulaires des cartes une protection adéquate contre toute utilisation frauduleuse. Les principales mesures qu'elles énoncent sont les suivantes :

– aucun commerçant ne peut exécuter quelque transaction que ce soit sans l'accord exprès du titulaire ;

(3) À l'origine, le législateur craignait la répercussion des droits par les commerçants sur la totalité des clients, indépendamment du mode de paiement, et donc la pénalisation des clients payant comptant.

– les émetteurs des cartes ne peuvent pas tenir pour responsables les titulaires qui communiquent leur numéro de carte (lequel n'est pas secret, à la différence du code) ;

– en cas de contestation d'une transaction par le titulaire d'une carte, l'opération doit être suspendue et le compte recrédité si la transaction a déjà été enregistrée.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

ESPAGNE

Il existe peu de dispositions législatives et réglementaires destinées spécifiquement à garantir la sécurité des transactions réalisées par carte bancaire. La plupart des règles applicables sont des règles générales, qui résultent notamment du droit des contrats et du droit de la consommation. Cependant, depuis qu'elle a été modifiée par la loi 47/2002 du 19 décembre 2002, adoptée pour transposer la directive 97/7 relative aux contrats à distance, **la loi 7/1996 du 15 janvier 1996 sur l'organisation du commerce de détail** comporte plusieurs mesures visant particulièrement la sécurité de la carte bancaire.

Les principales dispositions garantissant la sécurité des transactions réalisées par carte bancaire résultent de l'application par les établissements financiers, d'une part, du **code de bonne conduite du secteur bancaire européen 14 novembre 1990 relatif aux systèmes de paiement par carte** *(4)* (document n° 5) et, d'autre part, de **la recommandation 97/489 de la Commission européenne concernant les opérations effectuées au moyen d'instruments de paiement électronique.**

(4) La Fédération bancaire de la Communauté européenne, le Groupement des banques coopératives de la Communauté européenne et le Groupement européen des Caisses d'épargne, regroupées dans l'Association européenne du secteur du crédit (AESC), ont adopté ce code de bonne conduite pour répondre aux exigences des institutions communautaires.

I. LES DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES

1) Le cadre général

Aucune mesure générale ne vise spécifiquement la sécurité des cartes bancaires.

2) Les relations entre les établissements financiers et les titulaires de cartes bancaires

Elles sont déterminées par les contrats de mise à disposition des cartes bancaires, lesquels doivent notamment satisfaire aux conditions fixées par la loi de 1984 sur la défense des consommateurs et des usagers (clarté et simplicité de la rédaction…).

3) Les transactions individuelles

a) Le délai de rétractation

Lorsqu'un client achète à distance, il dispose d'un **délai de rétractation de sept jours ouvrables,** au cours desquels il peut renoncer à son achat sans pénalisation et sans avoir à indiquer de motif. Il doit seulement supporter les frais relatifs au retour de la marchandise au vendeur.

Cette disposition vise en particulier les achats réglés par carte bancaire.

b) Le remboursement de tout débit injustifié

En cas d'utilisation frauduleuse de la carte bancaire lors d'une opération de vente à distance, le titulaire de la carte peut demander l'annulation immédiate de la transaction. Le remboursement doit être effectué dans les plus brefs délais.

La preuve de l'utilisation frauduleuse d'une carte bancaire incombe à l'établissement de crédit.

4) Les mesures pénales

a) La fabrication et la falsification des cartes bancaires

La fabrication, la distribution et l'utilisation de fausses cartes bancaires relèvent du **même article du code pénal que la falsification de la monnaie fiduciaire**. Ces infractions sont donc sanctionnées par une peine de prison dont la durée est comprise entre huit et douze ans. Alors que, en cas de falsification de la monnaie fiduciaire, la peine de prison est assortie d'une amende dont le montant s'élève au décuple du montant de la monnaie falsifiée, aucune amende n'est imposée lorsque l'infraction concerne une carte bancaire, car la détermination de la valeur de la falsification est alors impossible.

En juin 2002, le Tribunal suprême a décidé que la modification de la piste magnétique d'une carte bancaire était assimilable à la fabrication d'une fausse carte bancaire et tombait donc également sous le coup de l'article du code pénal punissant la falsification de la monnaie fiduciaire.

b) La fraude informatique

La plupart des autres infractions relatives à la carte bancaire (interception d'un numéro de carte par exemple) relèvent de l'article du code pénal sur la fraude informatique. Cet article vise en effet tous les transferts de patrimoine réalisés par des moyens informatiques à l'insu et au détriment d'un tiers. Les contrevenants sont passibles d'une peine de prison dont la durée varie en fonction de l'importance de la fraude, mais qui est d'au moins six mois.

II. LES AUTRES MESURES

1) Les mesures prises par le secteur bancaire

a) Le code de bonne conduite

Les établissements financiers se réfèrent au code de bonne conduite du secteur bancaire européen du 14 novembre 1990 relatif aux systèmes de paiement par carte, qui détermine dans une large mesure les relations entre les établissements financiers et les titulaires de cartes bancaires.

- **La mise en garde des titulaires de cartes bancaires**

Les titulaires d'une carte bancaire ont l'obligation de prendre toutes les mesures raisonnables pour éviter l'utilisation frauduleuse de leur carte. Ils doivent

notamment éviter de conserver par écrit leur numéro de code sur la carte ou sur un document joint à celle-ci.

- **La limitation de responsabilité des titulaires de cartes bancaires**

En cas de perte, de vol ou de copie de la carte, la responsabilité du titulaire est engagée jusqu'au moment de la notification à l'établissement financier émetteur, mais à hauteur de 150 € seulement, sauf s'il a agi frauduleusement ou avec une extrême négligence. De plus, la charge de la preuve de la fraude ou de la négligence du titulaire pèse sur l'établissement financier émetteur de la carte.

Si le détenteur de la carte n'a pas informé sa banque du vol, de la perte ou de la copie de celle-ci, sa responsabilité est engagée. Toutefois, une limitation peut être déterminée contractuellement, suivant les termes de la recommandation 97/489. Elle n'est appliquée que si le titulaire de la carte n'a pas commis de négligence grave.

Dans la pratique, la plupart des établissements financiers ne respectent pas les termes de la recommandation 97/489 et incluent dans leurs documents contractuels des clauses abusives de limitation de leur responsabilité. La Banque d'Espagne déplore cette « *mauvaise pratique* » généralisée, qui conduit les titulaires de cartes bancaires à porter certaines affaires devant les tribunaux.

- **La fourniture aux titulaires de cartes bancaires d'informations relatives aux opérations réalisées**

Les titulaires de cartes bancaires doivent recevoir un relevé des opérations réalisées au moyen de leur carte.

Ils peuvent également recevoir un relevé sommaire immédiatement après la transaction.

b) Les autres mesures prises par le secteur bancaire

L'annexe VI de la **circulaire 8/1990 du 7 septembre 1990 de la Banque d'Espagne** précise qu'un relevé des transactions effectuées au moyen d'une carte de paiement doit être adressé régulièrement au client. La périodicité de cet envoi est déterminée contractuellement.

2) Les recommandations des associations de consommateurs

La plupart des cartes bancaires ne possédant pas de puce, il est recommandé aux commerçants de demander aux clients leur carte d'identité, de la comparer avec la carte bancaire, de vérifier que les deux documents sont bien ceux

du titulaire et enfin contrôler la signature du reçu, qui doit être identique à celle figurant sur la carte bancaire.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

ROYAUME-UNI

Il existe peu de dispositions législatives et réglementaires destinées spécifiquement à garantir la sécurité des transactions réalisées par carte bancaire : le **règlement sur la protection des consommateurs**, adopté en 2000 pour transposer la directive 97/7, comprend quelques mesures, mais elles valent seulement pour les ventes à distance.

Les principales règles applicables figurent dans le **code de bonne conduite des banques de mars 2003** (document n° 6), dont l'un des objectifs essentiels consiste à garantir un « *système bancaire et de paiements sûr et fiable* ». Bien que conclu sur une base volontaire, le code de bonne conduite s'impose à tous les signataires, c'est-à-dire à tous les établissements financiers.

Par ailleurs, les professionnels, tant du secteur bancaire que de la vente, ont pris diverses dispositions pour améliorer la sécurité des transactions réalisées par carte bancaire.

I. LES DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES

1) Le cadre général

À la suite de l'adoption, au cours de l'année 2000, de la loi régissant les pouvoirs d'enquête (*Regulation of Investigatory Powers Act*), qui a modifié les règles applicables à l'interception des communications, **une force de police spécialisée dans la lutte contre les infractions commises grâce à Internet** a été créée. Cette force de police est **notamment compétente pour prévenir et détecter les fraudes à la carte bancaire.**

2) Les relations entre les établissements financiers et les titulaires de cartes bancaires

Pour l'essentiel, elles sont définies dans le code de bonne conduite, et non dans un texte législatif ou réglementaire.

3) Les transactions individuelles

a) Le délai de rétractation

Le règlement sur la protection du consommateur en matière de **vente à distance**, adopté en 2000 pour transposer la directive 97/7, prévoit un délai de rétractation de **sept jours**.

b) Le remboursement de tout débit injustifié

Le règlement sur la protection du consommateur en matière de **vente à distance** dispose que le consommateur peut demander l'annulation des transactions réalisées frauduleusement à l'aide de sa carte. Son compte doit ensuite être recrédité du montant des achats. C'est à l'établissement financier qu'il appartient de prouver que la transaction a été réalisée de façon régulière lorsque le titulaire de la carte demande l'application de cette mesure.

4) Les mesures pénales

La loi de 1981 sur la contrefaçon et la falsification prévoit explicitement le cas des cartes bancaires : le fait de détenir sciemment de fausses cartes, avec l'intention de les utiliser ou de faire en sorte qu'un tiers les utilise, constitue une infraction, tout comme le fait de détenir du matériel destiné à fabriquer de fausses cartes.

Cette infraction, nécessairement jugée sur acte d'accusation *(5)*, est sanctionnée d'une **peine de prison**, dont la durée maximale peut atteindre dix années.

(5) Par opposition aux infractions susceptibles d'être jugées selon une procédure sommaire par des juges non professionnels, les infractions qui font l'objet d'un acte d'accusation sont jugées par la Crown Court *: la culpabilité est établie par un jury populaire et la peine est déterminée par un magistrat professionnel.*

II LES AUTRES MESURES

1) Les mesures prises par le secteur bancaire

a) Le code de bonne conduite des banques

Il inclut plusieurs dispositions, qui, dans les autres pays, font l'objet d'une loi, en particulier les dispositions sur la limitation de responsabilité des titulaires de cartes bancaires.

- **La limitation de la responsabilité des titulaires de cartes bancaires**

Dans la mesure où le titulaire d'une carte respecte les règles de précaution qui lui ont été communiquées et ne commet aucune fraude, sa responsabilité ne peut pas être engagée pour plus de 50 £ .

En effet, le code de bonne conduite limite la responsabilité des détenteurs de cartes bancaires à 50 £ (soit environ 80 €) en cas d'utilisation du code secret par un tiers avant que le détenteur de la carte n'ait indiqué la perte ou le vol de celle-ci à sa banque. Ce plafond s'applique à l'ensemble des opérations effectuées par le tiers, et non pas à chacune des transactions.

De plus, le code de bonne conduite exclut toute responsabilité du titulaire dans les deux cas suivants :

– la carte a été utilisée avant qu'il ne l'ait reçue ;

– les données de la carte ont été utilisées pour régler un achat fait en dehors de la présence du détenteur.

En revanche, en cas de grossière négligence, le titulaire de la carte voit sa responsabilité engagée sans limite.

Cette limitation de la responsabilité est assortie d'une clause sur la charge de la preuve : pour que la responsabilité du titulaire de la carte soit engagée sans limite, il revient à l'établissement signataire du code de bonne conduite de prouver que le titulaire n'a pas agi avec le soin requis ou qu'il a fraudé.

- **La mise en garde des titulaires de cartes bancaires**

Le code de bonne conduite se fixe pour objectif de fournir aux clients toutes les informations requises dans un langage « *clair* ». Il attire l'attention des titulaires de cartes bancaires sur la nécessité de prendre des **précautions** (ne pas

communiquer son code secret à un tiers, ne pas l'écrire, prévenir sa banque le plus vite possible en cas de vol…).

b) Les autres mesures prises par le secteur bancaire

Préoccupée par le développement de la fraude aux cartes, qu'elle estimait à 165 millions de livres pour 1992, à 317 millions pour 2000 et à 411,4 millions pour 2001, **l'APACS** (*Association for Payment Clearing Services*), qui regroupe la plupart des banques et des établissements financiers, s'efforce de lutter contre ce phénomène, notamment en collaborant avec la police, le ministère de l'Intérieur et tous les organismes chargés, à un titre ou à un autre, de la prévention des infractions.

Elle a également développé l'information sur la fraude. Ainsi, son site Internet www.cardwatch.org.uk comporte des renseignements pratiques destinés aux détaillants, aux consommateurs et aux forces de police.

L'APACS a progressivement imposé la multiplication des autorisations préalables aux règlements par carte : elles représentaient 10 % de toutes les transactions réalisées par carte bancaire au début des années 70 et sont passées à 90 % actuellement.

De plus, **au cours de l'année 2002**, elle a pris **deux mesures importantes** : elle a décidé le remplacement progressif des cartes à piste magnétique par des **cartes à puce** et a contribué à la création, en collaboration avec le ministère de l'Intérieur, d'un **corps de police spécialisé**.

- **La modernisation des cartes bancaires**

En février 2002, l'APACS a annoncé le remplacement progressif des quelque 100 millions de cartes bancaires en circulation dans le pays par des cartes à puce. L'opération devrait être achevée en **2005**.

Cette mesure vise principalement à réduire la fraude consistant à recopier les pistes magnétiques, qui s'est particulièrement développée. Son coût, estimé à 107,1 millions de livres pour 2000 et à 160,4 millions pour 2001, a été réduit à 148,5 millions en 2002.

- **La création d'un corps de police spécialisé**

En avril 2002, **un corps de police spécialisé dans la lutte contre la fraude aux moyens de paiement, la DCPCU** (*Dedicated Cheque and Plastic Crime Unit*), a été créé à titre expérimental pour deux ans.

La DCPCU n'opère que sur le territoire de l'Angleterre et du Pays de Galles. Elle est financée à hauteur de 75 % par l'APACS. Elle rassemble des officiers de police et des experts issus de la banque.

À l'issue de la période d'expérimentation, une évaluation sera conduite. Cette unité spécialisée pourrait alors être créée définitivement.

2) Les mesures prises par les autres professionnels

En 1999, le gouvernement a demandé aux organismes de défense des consommateurs et aux fournisseurs de biens et de service en ligne d'élaborer une charte répondant aux besoins des consommateurs désireux de faire leurs achats sur Internet.

Une association sans but lucratif, **TrustUK,** a été créée avec l'appui du gouvernement. Elle délivre son agrément aux sites Internet qui se conforment à ses critères, parmi lesquels la **sécurité des paiements**.

LA SÉCURITÉ DES TRANSACTIONS RÉALISÉES PAR CARTE BANCAIRE

LISTE DES PRINCIPAUX TEXTES ANALYSÉS

Document n° 1	Union européenne – Directive 97/7/CE du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance
Document n° 2	Union européenne – Recommandation 97/489/CE de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique
Document n° 3	Belgique – Loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds
Document n° 4	Danemark – Loi du 31 mai 2000 sur «*certains moyens de paiement* » (langue originale)
Document n° 5	Espagne – Code de bonne conduite du secteur bancaire européen 14 novembre 1990 relatif aux systèmes de paiement par carte
Document n° 6	Royaume-Uni – Code bonne conduite des banques et établissements financiers (langue originale)