# N° 2992

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

ONZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 18 avril 2001.

# AVIS

PRÉSENTÉ

AU NOM DE LA COMMISSION DES FINANCES, DE L'ÉCONOMIE GÉNÉRALE ET DU PLAN (1), SUR LE PROJET DE LOI *relatif à la* **sécurité quotidienne**,

PAR M. JEAN-PIERRE BRARD,

Député.

(1) La composition de cette commission figure au verso de la présente page.

Voir les numéros : **2938** et **2996**

**Ordre public.**

*La Commission des finances, de l'économie générale et du plan est composée de :*
M. Henri Emmanuelli, *président* ; M. Michel Bouvard, M. Jean-Pierre Brard, M. Yves Tavernier, *vice-présidents* ; M. Pierre Bourguignon, M. Jean-Jacques Jégou, M. Michel Suchod, *secrétaires* ; M. Didier Migaud, *rapporteur général* ; M. Maurice Adevah-Poeuf, M. Philippe Auberger, M. François d'Aubert, M. Dominique Baert, M. Jean-Pierre Balligand, M. Gérard Bapt, M. François Baroin, M. Alain Barrau, M. Jacques Barrot, M. Christian Bergelin, M. Éric Besson, M. Alain Bocquet, M. Augustin Bonrepaux, M. Jean-Michel Boucheron, Mme Nicole Bricq, M. Christian Cabal, M. Jérôme Cahuzac, M. Thierry Carcenac, M. Gilles Carrez, M. Henry Chabert, M. Didier Chouat, M. Alain Claeys, M. Charles de Courson, M. Christian Cuvilliez, M. Arthur Dehaine, M. Jean-Pierre Delalande, M.Francis Delattre, M. Yves Deniaud, M. Michel Destot, M. Patrick Devedjian, M. Laurent Dominati, M. Julien Dray, M. Tony Dreyfus, M. Jean-Louis Dumont, M. Daniel Feurtet, M. Pierre Forgues, M. Gérard Fuchs, M. Gilbert Gantier, M. Jean de Gaulle, M. Hervé Gaymard, M. Jacques Guyard, M. Edmond Hervé, M. Pierre Hériaud, M. Jean-Louis Idiart, Mme Anne-Marie Idrac, M. Michel Inchauspé, Jean-Pierre Kucheida, M. Marc Laffineur, M. Jean-Marie Le Guen, M. Maurice Ligot, M. François Loos, M. Alain Madelin, M. Jean-Michel Marchand, Mme Béatrice Marre, M. Louis Mexandeau, M. Gilbert Mitterrand, M. Pierre Méhaignerie, M. Jean Rigal, M. Alain Rodet, M. José Rossi, M. Nicolas Sarkozy, M. Georges Sarre, M. Philippe Séguin, M. Georges Tron, M. Jean Vila.

# SOMMAIRE

MESDAMES, MESSIEURS,

Depuis plusieurs mois, la sécurité des cartes bancaires semble mise en cause, ce qui suscite une vive inquiétude dans le grand public et conduit les pouvoirs publics à réagir.

La forte médiatisation de « l'affaire Humpich », en 1999, a pu laisser supposer que les « secrets » de la carte à puce avaient été cassés, laissant la voie ouverte à de multiples piratages. Les titres de la presse n'ont pas été les seuls éléments à accréditer cette vision : dans l'un des attendus du jugement de M. Serge Humpich, en date du 25 février 2000, la 13ème chambre correctionnelle du tribunal de grande instance de Paris n'hésite pas à affirmer que « *cette fraude informatique, par la menace qu'elle fera courir* ***sur l'ensemble des transactions par cartes bancaires****, a troublé* ***gravement*** *l'ordre public* ».

De tels propos ne pouvaient manquer d'alerter les consommateurs, d'autant que, parallèlement, le Conseil de sécurité intérieure du 30 janvier 2001 annonçait une amplification de la fraude concernant les cartes bancaires.

Le Gouvernement, par l'entremise de Mme Marylise Lebranchu, alors secrétaire d'Etat aux petites et moyennes entreprises, au commerce et à l'artisanat, s'est saisi du dossier, en avril 2000, en organisant une table ronde et en annonçant la création d'un groupe de travail rattaché au Conseil national de la consommation.

Il était légitime que la représentation nationale se saisisse également de ce problème.

Les membres du groupe communiste et apparentés ont déposé, le 17 mai 2000, une proposition de résolution tendant à la création d'une commission d'enquête sur la sécurité des cartes bancaires (n° 2397).

Néanmoins, votre Rapporteur pour avis qui avait également été désigné, par la Commission des finances, de l'économie générale et du Plan, comme rapporteur de la proposition de résolution précitée, a jugé plus opportun, en définitive, d'en proposer le rejet, car « *la formule de la commission d'enquête, par sa solennité et son caractère exceptionnel, serait de nature à troubler l'opinion, en laissant à penser que l'Assemblée nationale estime établie l'existence d'un problème grave, affectant la sécurité des paiements par cartes bancaires* » (rapport n° 2530).

Ces conclusions de rejet, approuvées par la Commission des finances le 28 juin 2000, étaient, cependant, assorties d'un engagement du Président de ladite commission, visant à désigner, à l'automne 2000, un rapporteur d'information sur le même sujet, considérant que les auditions prévues devaient permettre d'éclairer l'Assemblée nationale sans qu'il fut nécessaire d'avoir recours à la procédure de la commission d'enquête.

Cet engagement a été tenu et, lors de sa réunion du 17 octobre 2000, la Commission des finances m'a nommé rapporteur d'information sur les cartes bancaires. Ce travail, qui n'a pu être engagé qu'à compter de décembre 2000, après l'adoption des projets de loi de finances, a déjà permis d'auditionner de nombreux intervenants (Groupement des cartes bancaires, banques, associations de consommateurs ou de commerçants, représentants des administrations concernées, industriels…).

La présentation par le Gouvernement, le 22 février 2001, de plusieurs dispositions législatives relatives à la sécurité des cartes de paiement devant être insérées dans le projet de loi relatif à la sécurité quotidienne (n° 2938), m'a conduit à demander à être nommé Rapporteur pour avis des articles 7 à 12 et 16 dudit projet de loi.

Ce rapport pour avis se substitue donc au rapport d'étape que j'avais envisagé de présenter dans le cadre de ma mission d'information, qui devrait se conclure par un rapport spécifique au cours du second semestre.

Dans l'immédiat, le présent rapport pour avis permet de dresser plusieurs constats :

– les cartes bancaires constituent un moyen de paiement usuel et le support d'un secteur de pointe de l'industrie française ; elles doivent donc bénéficier du maximum de sécurité ;

– les événements de ces derniers mois ont pu faire naître des doutes sur l'adéquation entre le niveau de protection des cartes bancaires et les capacités techniques actuelles des fraudeurs, même s'il convient de relativiser le taux de fraude constaté et de réaffirmer énergiquement que la carte à puce demeure incontestablement un moyen de paiement très fiable ;

– les mesures de sécurisation figurant dans le présent projet de loi se révèlent pertinentes, d'autant qu'elles sont complétées par des engagements souscrits par les établissements de crédit et le Conseil du commerce de France et qu'elles s'inscrivent dans une importante mobilisation internationale visant à faciliter la lutte contre les fraudeurs ;

– sur le plan strictement législatif, le dispositif proposé peut néanmoins être précisé et complété.

## CHAPITRE PREMIER

## LES CARTES BANCAIRES DOIVENT BENEFICIER DU NIVEAU MAXIMUM DE SECURITE

La nécessité absolue de sécuriser au mieux les cartes bancaires apparaît une évidence. Pourtant, les faits l'ont prouvé, le Groupement des cartes bancaires et ses membres, c'est-à-dire les banques, ont parfois perdu de vue cet objectif primordial. Cette négligence est d'autant plus condamnable que les cartes bancaires constituent dorénavant un moyen de paiement usuel et que la technologie de la puce représente un secteur de pointe de l'industrie française.

### I.- UN MOYEN DE PAIEMENT USUEL

Aux termes de l'article 4 de la loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit : « *Sont considérés comme moyens de paiement tous les instruments qui, quel que soit le support ou le procédé technique utilisé, permettent à toute personne de transférer des fonds* ». Les moyens de paiement sont répartis en deux grandes catégories : d'une part, la monnaie fiduciaire (billets et pièces métalliques) qui se caractérise par le fait que le moyen de paiement se confond avec l'instrument monétaire ; d'autre part, la monnaie scripturale pour laquelle le rôle d'instrument monétaire est assuré par le compte bancaire. Dans ce dernier cas, en effet, les moyens de paiement vont déclencher le paiement en donnant l'ordre à l'établissement bancaire qui détient le compte de transférer des fonds sur le compte de son créancier par une double opération : une inscription au débit d'un compte (celui du payeur) et une inscription au crédit d'un autre compte (celui du payé). Ainsi, la monnaie scripturale peut se définir comme une somme d'argent inscrite sur un compte bancaire et qui circule de compte à compte à l'aide d'instruments de paiement scripturaux comme le chèque, le virement ou la carte bancaire.

En trois décennies, la carte bancaire s'est imposée, grâce aux avantages qui lui sont propres, comme l'un des principaux moyens de paiement utilisés en France et a connu une importante diversification.

## A.- UN INSTRUMENT RECENT ET REPONDANT A UNE DEMANDE

### 1.- Aperçu historique

Dans son roman « *La nuit des temps* » publié en 1968, René Barjavel imaginait une civilisation disparue où « *chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandé* ».

A la même époque, cinq grandes banques françaises (le Crédit lyonnais, la Société générale, la Banque nationale de Paris, le Crédit industriel et commercial, ainsi que le Crédit commercial de France) se regroupaient pour le lancement de la « carte bleue ».

Destinée au départ à concurrencer les cartes « American express » et « Diners club », cette carte, initialement réservée à une clientèle sélectionnée, se distinguait des autres cartes – y compris des cartes bancaires américaines – par le fait que le débit des paiements effectués par le titulaire était réalisé sur son compte sans que l'émission d'un moyen de paiement - chèque ou avis de prélèvement du montant de la facture envoyée périodiquement au porteur par l'émetteur de la carte – fût nécessaire. L'objectif fondamental de cette innovation était effectivement la réduction du nombre de chèques, instrument de paiement dont la gratuité est imposée par la loi.

L'apparition de la technique des pistes magnétiques incorporées au dos des cartes devait, en 1971, permettre d'associer à la « carte bleue » une fonction de retrait de billets dans les automates bancaires ; la diffusion de cette carte s'en trouva élargie.

En 1971, fut créé le Groupement d'intérêt économique « Carte bleue » auquel devaient se rallier d'autres banques que les banques fondatrices et qui devint, en 1976, membre de « Visa international », ce qui ouvrit aux porteurs de la « carte bleue » la possibilité de régler leurs achats à l'étranger.

L'adhésion, en 1983, des banques populaires, des caisses d'épargne et de prévoyance et des chèques postaux au groupement « carte bleue » devait marquer une étape décisive dans cette évolution vers un rassemblement des émetteurs de cartes gestionnaires de dépôts à vue. A la veille de l'accord national de 1984, ne subsistaient plus que trois réseaux émetteurs de cartes bancaires : le réseau du Crédit agricole, émetteur de la

« carte verte » (7,5 millions de cartes), dont les caractéristiques s'étaient peu à peu rapprochées de celles de la « carte bleue », celui du Crédit mutuel (1,3 million de cartes), celui de la « carte bleue » (5 millions de cartes), regroupant tous les émetteurs n'appartenant pas aux deux précédents réseaux.

En signant un protocole d'accord du 31 juillet 1984, ces trois réseaux s'engageaient à constituer en commun un groupement d'intérêt économique et à réaliser entre eux une « interbancarité » totale, tant en ce qui concerne la fonction de retrait de billets, qu'en ce qui concerne la fonction de paiement dans le commerce, permettant à tout porteur d'une carte entrant dans la gamme des cartes du groupement d'accéder, quel que soit l'établissement émetteur, à tous les appareils de retrait automatique de billets mis en place par les membres du groupement et de régler ses achats dans tous les commerces jusqu'alors affiliés à l'un des réseaux signataires du protocole. La mise en compatibilité des automates bancaires et du matériel de traitement en place chez les commerçants permettant la réalisation de cet objectif fut achevée le 1er juillet 1985 pour la fonction de retrait, et le 1er novembre 1985 pour la fonction de paiement.

La fraude relevée sur la carte bleue a conduit, en 1990, à renforcer la sécurité par la mise en place sur la carte d'un microprocesseur (la puce), dont l'utilisation est généralisée depuis 1992.

## 2.- Avantages de la carte bancaire

Conçue à l'origine pour réduire le nombre de chèques émis, la carte bancaire n'a pas encore, loin de là, atteint son objectif, même si – comme cela sera indiqué ci-après – sa part parmi les instruments de paiement, ne cesse de progresser au détriment du chèque. Ce succès peut s'expliquer par les avantages qu'elle procure aux différents utilisateurs.

### *a) Les porteurs*

La carte permet à son titulaire d'effectuer des achats chez les commerçants affiliés, sur simple signature de la facture ou composition du code confidentiel. Le porteur est ainsi dispensé de prouver son identité.

S'agissant toujours de la fonction « achats », le porteur peut également profiter du crédit gratuit offert par le paiement différé, solution choisie par 98% des titulaires.

La carte permet, par ailleurs, au porteur d'opérer des retraits rapides de fonds dans les distributeurs automatiques de billets (DAB).

L'interbancarité, mise en place en 1984, autorise le retrait d'espèces auprès de n'importe quel DAB et le règlement d'achats chez tout commerçant ou prestataire de services affichant la marque « CB ». En outre, les accords passés avec Visa et Europay Mastercard, dans le cadre de ce que l'on appelle l'interopérabilité internationale, rendent possible l'utilisation de la carte « CB » dans plus de 200 pays.

Enfin, certaines cartes offrent des services supplémentaires (assurance sur la vie, réductions dans certains magasins, dispense de cautionnement pour la location de véhicules automobiles…).

*b) Les commerçants*

La plupart des cartes de paiement garantissent au commerçant qui les accepte le règlement de ses factures dans la limite d'un certain montant (par jour et/ou par commerçant ou machine imprimante).

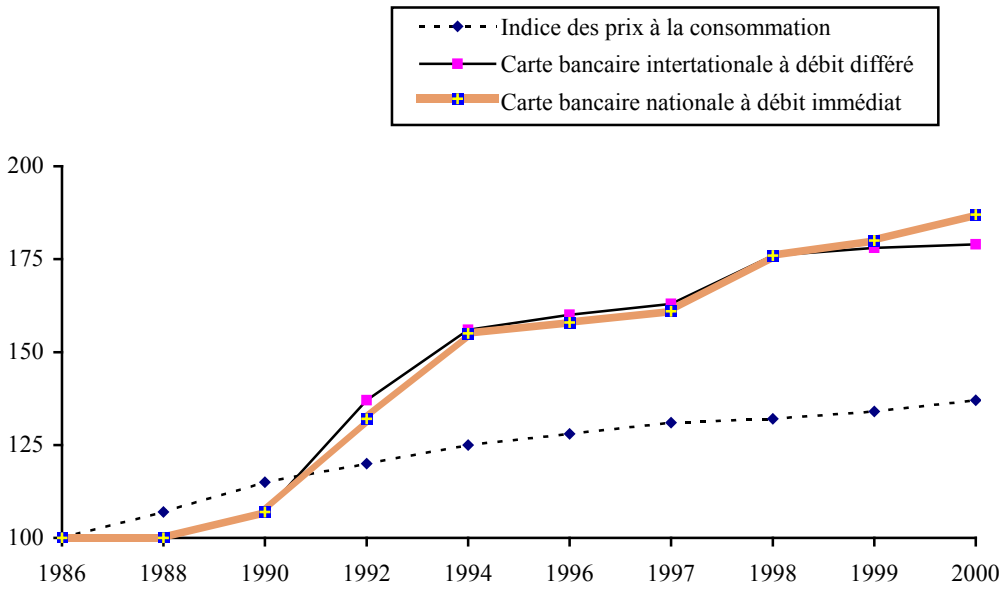
L'acceptation des cartes entraîne également une simplification des opérations de comptabilisation en fin de journée.

*c) Les banques*

La carte bancaire constitue le seul instrument de paiement donnant lieu à une rémunération depuis sa création.

A cet égard, il importe d'ailleurs de souligner que le montant annuel des cotisations à la charge des porteurs de cartes a sensiblement progressé ces dernières années, selon les statistiques de l'Institut national de la consommation. Ainsi, le prix de la carte nationale à débit immédiat aurait progressé de 91% de 1986 à 2000, tandis que celui de la carte internationale à débit différé aurait augmenté de 82% durant la même période.

**EVOLUTION DES PRIX DES CARTES BANCAIRES**




*Source : INC Hebdo n° 1123 du 5 mai 2000*
*« L'indice des prix des services bancaires aux particuliers ».*

On peut observer qu'aux Etats-Unis, la concurrence entre émetteurs de cartes bancaires est quasiment parvenue à supprimer la facturation de cotisations annuelles.

## B.- UNE FORTE DIVERSIFICATION

Les développements précédents ont fait usage indistinctement des termes « carte de paiement », « carte bancaire » et « carte CB », généralement considérés comme synonymes dans la pratique quotidienne. Il convient, à ce stade, d'adopter une approche plus juridique et de définir précisément ces termes [(1)].

L'exercice n'est pas aisé, car le secteur est en mutation rapide, les informations parcellaires et de multiples critères de classement peuvent être retenus, dont aucun n'est, à vrai dire, pleinement satisfaisant : le statut de

*(1) Les informations fournies par la suite s'inspirent très largement d'une note de la direction des services juridiques de la Banque de France sur « la typologie des cartes de paiement », datée du 13 décembre 2000.*

l'émetteur (établissement de crédit ou non), la qualité du porteur (particulier ou entreprise), la fonction de la carte (retrait, paiement, crédit), la sphère d'utilisation (carte mono ou multi prestataire, nationale ou internationale), les caractéristiques techniques (carte à piste, à puce, carte à autorisation systématique, carte préchargée). Il semble, toutefois, pertinent, dans le cadre d'une approche globale, de faire, en raison des dispositions légales, une première distinction entre cartes émises par des établissements de crédit et cartes émises par des entreprises de droit commun.

En application de la loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit, seuls les établissements de crédit, c'est-à-dire des personnes morales bénéficiant d'un agrément, peuvent, sauf exceptions, mettre à la disposition de la clientèle ou gérer des moyens de paiement, à titre de profession habituelle (articles premier, 15, 71-2 et 71-3).

Cependant, aux termes de l'article 12 de ladite loi bancaire, une entreprise, quelle que soit sa nature, peut, entre autres :

« *1° Dans l'exercice de son activité professionnelle consentir à ses contractants des délais ou avances de paiement ;*

*5° Emettre des bons et cartes délivrés pour l'achat auprès d'elle d'un bien ou d'un service déterminé…* ».

Par conséquent, deux grandes catégories de cartes peuvent être distinguées : celles qui sont émises par des établissements de crédit et celles qui sont émises par des entreprises non dotées d'un tel statut, mais qui agissent dans le cadre de l'article 12-5° de la loi bancaire.

A s'en tenir strictement à la définition donnée par l'article 57-1 du décret-loi du 30 octobre 1935 unifiant le droit en matière de chèques et relatif aux cartes de paiement – article introduit par loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement et désormais codifié à l'article L. 132-1 du code monétaire et financier –, seules les premières mériteraient le qualificatif de carte de retrait ou de paiement puisque l'article 57-1 définit celles-ci comme des cartes émises par un établissement de crédit ou un organisme visé à l'article 8 de la loi bancaire [(1)], la carte de retrait « *permettant exclusivement à son titulaire de retirer des fonds* » et la carte de paiement « *permettant à son titulaire de retirer et de transférer des fonds* ». Il s'agit donc d'une définition qui caractérise la carte selon la qualité de son émetteur et son objet.

---

*(1) Trésor public, Banque de France, services financiers de La Poste, Institut d'émission d'outre-mer, Institut d'émission des départements d'outre-mer et Caisse des dépôts et consignations.*

Compte tenu de leur objet, il aurait pu paraître logique de qualifier aussi de cartes de paiement les cartes émises par les entreprises utilisant le régime dérogatoire instauré par l'article 125° de la loi bancaire, toutefois la fonction de retrait ne leur est pas ouverte. Le plus souvent appelées cartes privatives et parfois cartes purement privatives, elles sont en principe des cartes mono prestataires (ou mono enseignes), c'est-à-dire utilisables auprès d'une seule entreprise ou d'une seule enseigne.

Cependant, l'expression carte privative est assez fréquemment utilisée pour désigner aussi une carte émise et gérée par un établissement de crédit en faveur d'une entreprise donnée, voire toute carte émise par un établissement de crédit mais qui n'est pas une carte bancaire « CB ». Cette dernière est émise par un établissement de crédit adhérent du GIE cartes bancaires « CB », porte le logo « CB » et est acceptée dans tout le réseau des adhérents et chez les accepteurs accrédités « CB », ce qui amène à la qualifier de carte interbancaire et de carte universelle.

Par commodité de langage, il serait sans doute souhaitable de parler de « cartes privatives » pour les seules cartes émises par des non-établissements de crédit et de « cartes bancaires » pour les cartes émises par des établissements de crédit, quelle que soit la nature de leur agrément (banque, société financière, institution financière spécialisée…) et même lorsque la carte est mono prestataire.

### 1.- Les cartes émises par des établissements de crédit ou des institutions assimilées

Ce sont, au sens large défini ci-avant, des cartes bancaires de retrait ou de paiement.

Elles méritent le qualificatif de cartes de crédit si le titulaire de la carte bénéficie d'une ouverture de crédit lui permettant de régler l'émetteur à l'issue d'un certain délai, étant précisé que l'octroi d'un différé de paiement inférieur ou égal à quarante jours n'est pas assimilé à une opération de crédit [(1)].

On rencontre aussi l'expression « cartes accréditives », qui a jadis servi à désigner les cartes émises par les sociétés *Diners* et *American Express* avant qu'elles ne soient contraintes, en vertu de la loi de 1984, d'adopter un statut d'établissement de crédit [(2)]. Cette expression a vocation

*(1) Avis n° 67-06 du 28 juin 1968 du Conseil national du crédit.*

*(2) Avant la mise en vigueur de la loi bancaire de 1984, l'émission et la gestion de moyens de paiement ne figuraient pas parmi les opérations de banque et n'impliquaient donc pas un agrément pour les réaliser.*

à s'appliquer à toute carte émise par un établissement de crédit, acceptée par des commerçants accrédités et dont le titulaire règle l'émetteur par le débit d'un compte bancaire non géré par l'émetteur. C'est à vrai dire la situation de la quasi-totalité des cartes émises par les établissements de crédit spécialisés. Le porteur d'une carte émise par Cetelem, Cofinoga, Finaref, etc. reçoit un relevé des paiements effectués au cours d'une période donnée et règle l'émetteur par le débit du compte (avis de prélèvements, chèques…) qu'il détient par ailleurs.

Les cartes émises par les établissements de crédit ou des institutions assimilées peuvent être réparties en deux catégories principales : les cartes bancaires « CB »,*stricto sensu* et les autres cartes bancaires.

*a) Les cartes bancaires « CB »*

Une carte bancaire « CB » est une carte émise dans les conditions fixées par le Groupement des cartes bancaires « CB », le titulaire de la carte ayant notamment signé avec l'émetteur un contrat, dit porteur, dont le contenu reprend pour l'essentiel un contrat type élaboré par ledit groupement.

Fin 2000, on dénombrait 40,9 millions de cartes « CB » dont 5,3 millions de cartes « CB » nationales et 35,6 millions de cartes internationales se ventilant elles-mêmes en 19,3 millions de cartes « CB » Visa et 16,3 millions de cartes « CB » Eurocard Mastercard.

Les cartes sur lesquelles figurent le logo « CB » sont émises par des établissements membres du GIE cartes bancaires « CB » et sont acceptées par chacun d'entre eux. Le nom de l'émetteur est noté sur le recto et le verso de la carte, qui porte aussi sur le seul recto les mentions Carte Bleue ou Eurocard et, le cas échéant, les marques Visa ou Eurocard-Mastercard.

La typologie des cartes bancaires « CB » peut être rapidement dressée.

• **Cartes « CB » nationales**

Leur nombre est en réduction constante : 5,3 millions au 1er janvier 2001, contre 6,27 millions au 1er janvier 2000. Elles sont acceptées en France métropolitaine, dans les DOM, les TOM et Monaco.

*– Cartes « CB » de retrait*

Elles permettent uniquement de retirer des espèces dans les 35.000 DAB « CB » en France. On en recense 540.000.

*– Cartes « CB » de paiement*

Les 5.730.000 cartes en circulation permettent le paiement chez les 623.000 accepteurs « CB » en France, ainsi que des retraits d'espèces dans les DAB et les agences. La Carte Bleue nationale et la carte Eurocard peuvent être à usage personnel ou professionnel, à débit immédiat ou à débit différé, à autorisation systématique ou non (dans cette dernière hypothèse, elles sont des cartes dites classiques).

Les retraits dans les DAB sont toujours imputés au jour le jour au débit du compte du titulaire. En revanche, les paiements, chez les commerçants peuvent être imputés au compte soit au fur et à mesure des paiements (cartes à débit immédiat), soit après un certain délai (40 jours maximum afin que l'opération ne soit pas qualifiée de crédit) dans le cas des cartes à débit différé. En général, les paiements réalisés sur une période de 30 jours sont débités au compte en une seule fois à une date préétablie. La cotisation pour les cartes à débit différé est supérieure à celle qui est due pour les cartes à débit immédiat.

• **Cartes « CB » internationales**

Elles sont acceptées en France dans le réseau « CB » et à l'étranger dans le réseau international (Visa ou Mastercard) auquel chaque carte est affiliée.

*– Cartes « CB » de retrait*

Il s'agit des 930.000 cartes « CB » Plus (réseau visa Plus) et des 2.600.000 cartes « CB » Cirrus (réseau Eurocard Mastercard).

La carte Plus a la particularité d'être assortie d'un plafond personnalisable de retraits d'espèces. Elle a aussi vocation à être proposée à des mineurs âgés d'au moins douze ans (après accord du représentant légal).

*– Cartes « CB » à autorisation systématique*

Sont en circulation en France 485.000 cartes Visa Electron dont la commercialisation a débuté en 1999 et 690.000 cartes « CB » Maestro. Cette dernière – qui est un produit conçu en 1992 par Maestro International, société codétenue par Europay International et Mastercard International – compte 158 millions de porteurs européens et est utilisable auprès de 4,6 millions de terminaux de paiement dans le monde.

Le retrait d'argent et le paiement chez un commerçant sont systématiquement précédés d'une interrogation automatique du compte afin de vérifier qu'il est suffisamment approvisionné. Ce sont, par construction, des cartes à débit immédiat.

*– Cartes « CB » classiques*

Acceptées en France dans les mêmes conditions que les « CB » nationales, les cartes « CB » Visa (14,3 millions) et « CB » Eurocard Mastercard (10,7 millions) donnent en outre la possibilité d'effectuer des paiements et de retirer à l'étranger des espèces au sein du réseau respectif d'accepteurs et d'agences, soit environ 17,2 millions de commerçants et 560.000 DAB pour chacun des réseaux [(1)] qui, l'un et l'autre, revendiquent le titre de premier réseau mondial.

*– Cartes « CB » de prestige*

Elles offrent à leurs porteurs des capacités de retrait et de paiement plus importantes que les cartes classiques et des services accrus notamment en matière d'assurance. Un million de « CB » Visa Premier, 155.000 « CB » Gold Master Card et 68.000 Gold Affaires sont en circulation

*– Cartes « CB » professionnelles*

Ce sont des cartes personnelles à usage professionnel. On dénombre 210.000 cartes « CB » Visa Affaires et Visa Business et 170.000 cartes « CB » Business Card Mastercard.

*– Cartes Visa Travel Money*

Présentées par leurs promoteurs comme la « version électronique du chèque de voyage », elles permettent de retirer des devises dans les

*(1) Il y aurait un milliard de cartes Visa et 700 millions de cartes Mastercard en circulation à travers le monde.*

560.000 DAB Visa Plus, dans la limite du montant préalablement déposé à la banque.

*b) Autres cartes bancaires*

Leur nombre et leur variété sont difficiles à connaître, car aucun recensement statistique n'est effectué et car certains émetteurs ne publient aucune donnée sur le sujet. Sont évoqués, ci-après, la situation et les produits de quelques-uns uns des principaux émetteurs de cartes en France.

• **Les cartes « badges »**

Ce sont des cartes de retrait dont l'usage n'est possible qu'au sein du réseau de guichets de l'établissement de crédit émetteur. Elles sont parfois destinées à une clientèle spécifique, notamment les jeunes, telles les cartes Jeans-club de la BNP, Mozaic du Crédit agricole et Kit de la Société générale.

• **Les cartes Cetelem**

Banque spécialisée dans le crédit aux particuliers, qui appartient au groupe BNP Paribas, Cetelem est un des plus anciens et plus importants intervenants du secteur, qu'elle agisse sous sa propre bannière ou à travers de multiples partenariats. Elle détient 49% dans Finalion (Crédit Lyonnais) et Finama (Groupama), 44% dans Cofinoga (Galeries Lafayette), 40% dans S2P (filiale Carrefour), 34% dans Novacrédit (Banques populaires) et Covefi (3 Suisses), 15% dans Cofidis (3 Suisses), 50% dans Volvo Automobile Finance France, Loisirs finances (groupe Trigano) et Dartem (Darty), 51% dans Inchcape France Finance (Mazda), Fidem (groupe But), NorrskenFinance (Ikea), 39% dans Facet (Finaref)…

Elle gère de nombreuses cartes pour le compte de tiers, y compris des établissements de crédit (Allure du CIC, Satellis Aurore des Caisses d'Epargne, Libre cours du Crédit Lyonnais) et elle est le concepteur de la carte Aurore.

• **La carte Aurore**

Présentée par ses promoteurs comme une « carte de paiement à crédit », elle est diffusée auprès de 12 millions de personnes en Europe, dont 8,5 millions en France, et est acceptée par 152.000 commerçants ; elle mérite d'être signalée car elle est acceptée dans le réseau des DAB cartes bancaires « CB » alors qu'elle n'est pas un produit Carte bleue, Europay, Visa ou Eurocard Mastercard.

Elle a été créée par Cetelem. C'est désormais le GIE Aurore, constitué de dix entités (Banques populaires, Caisses d'épargne, GAN, Groupama, Cetelem…), qui gère ce produit.

**• Les cartes émises par Cofinoga et Soficarte**

Créée en 1968 en vue notamment de concevoir et de gérer des cartes de magasin, Cofinoga se présente comme le leader européen du crédit à la consommation. Son capital est détenu à 51% par le groupe Galeries Lafayette, 44% par Cetelem et 5% par BNP Paribas. Cofinoga a plus de 200 partenaires et travaille pour 80 enseignes.

Cofinoga émet des cartes acceptées par chacune des sociétés partenaires (30.000 points de vente). La carte Galeries Lafayette Cofinoga permet ainsi de régler des achats auprès du BHV, d'Avis, d'Air France, de la SNCF, de Total… Les cartes sont aussi admises dans certains centres commerciaux (Belle Epine, Parly 2…) et dans 84 « centres-villes» représentant 12.000 commerçants. Environ 200 DAB acceptent les cartes Cofinoga.

Cofinoga est le créateur du programme de fidélisation Points Ciel ; le plus important programme multi-enseignes : 2 millions d'adhérents et 35 enseignes.

De son côté, Soficarte, filiale à 100% de Cofinoga, émet des cartes qu'elle appelle « privatives mono-enseignes » et qui sont utilisables dans les seuls magasins de l'enseigne concerné (Habitat, Mr Bricolage, Ford, Audi, Club Méditerranée…).

En outre, Cofinoga vient de créer Agys, société destinée à développer des cartes multiservices, cartes à puce permettant le stockage de monnaie ou de points de fidélité. Elle était à l'origine du concept Vitavil, carte conférant à ses possesseurs des avantages offerts par les commerçants de centre-ville et les collectivités publiques.

Enfin, Cofinoga possède 45% du capital de la société financière Between (le solde étant détenu par BNP Paribas) qui a été créée en 1999 en vue de gérer des « cartes co-marketées » et ultérieurement « co-brandées » (sic). Between a ainsi émis une carte Banque de Bretagne et une carte Olympe pour l'Olympique de Marseille.

**• Les Cartes émises par Finaref**

Société financière créée à Roubaix en 1970, Finaref fait partie du groupe Pinault Printemps Redoute (PPR) et se présente comme le

précurseur du crédit permanent en France avec la carte Kangourou-La Redoute. Elle est un des acteurs importants de l'émission de cartes de crédit en France (7,5 millions de cartes en circulation). Elle émet en faveur des sociétés du groupe PPR les cartes suivantes : Kangourou (3,9 millions de cartes), Conforama (1,8 million), Printemps (0,75 million), FNAC (0,8 million)… Ces cartes, que Finaref qualifie de « privatives », sont aux couleurs de chacune des sociétés concernées, mais comportent le logo et les coordonnées de Finaref qui en est l'émetteur et le gestionnaire. Elles ne sont pas strictement privatives, car elles ne sont pas mono-prestataires. En effet, chacune d'entre elles est acceptée dans les autres sociétés du groupe : la carte FNAC est acceptée par La Redoute, Conforama…

La carte Conforama – gérée en pratique par Facet, filiale de Finaref – est en plus acceptée dans le réseau Aurore dont le logo apparaît sur la carte.

• **Les cartes Cofidis**

Société financière dont le capital est détenu par les 3 Suisses International (85%) et Cetelem (15%), Cofidis propose actuellement quatre « cartes distributeurs » :

– 4 étoiles, créée en 1985 pour financer l'achat à crédit auprès notamment des 3 Suisses France et de La Blanche Porte (3,7 millions de détenteurs) ;

– Ténor, carte « multivépéristes » acceptée par 17 enseignes (Joué Club, M6 Boutique, Linvosges…) ;

– Helline ;

– Cofidis Aurore en partenariat avec Cetelem.

• **La carte Accord**

Diffusée auprès de 1,4 million de porteurs, elle permet de régler des achats dans 2.000 points de vente constitués par 500 établissements des 15 enseignes du groupe Auchan-Mulliez (Auchan, Leroy Merlin, Norauto, Saint-Maclou…) et 1.500 commerçants installés dans les galeries marchandes.

• **La carte Pass**

Entre 1,5 et 2 millions de personnes seraient titulaires de la carte émise par S2P, société financière détenue par le groupe Carrefour (60%) et Cetelem (40%) et acceptée dans les magasins dudit groupe.

• **Les cartes Franfinance**

Etablissement de crédit appartenant au groupe Société générale, Franfinance émet des « cartes d'enseigne » en faveur d'entreprises de secteurs variés : Connexion, Mondial Moquette, BP fioul, Assu 2000, Nouvelles frontières, etc… Les chiffres de diffusion de ces produits ne sont pas publiés.

• **Les cartes *American Express***

Le nombre de porteurs de cartes de paiement et de crédit (personnel, platinium, Gold, corporate) d'*American Express* serait voisin de 500.000 en France.

*American Express* est désormais présent sur le marché des cartes co-marquées, par exemple avec la carte Air France-Accor ou la carte Peugeot, cette dernière est ainsi acceptée dans le réseau Peugeot, chez les partenaires de Peugeot et chez tous les commerçants accrédités Amex à travers le monde.

Signalons, en revanche, que la carte *Diners* a une diffusion restreinte en France (moins de 50.000) ; *Diners Club* de France n'est d'ailleurs plus agréé comme société financière.

En définitive, les montages multiples et divers qui sont mis en place dans le cadre de partenariats entre établissements de crédit et entreprises de droit commun, voire entre établissements de crédit, expliquent les difficultés à cerner de façon précise la situation actuelle en matière de cartes, situation très évolutive sous l'effet de multiples causes : restructuration des secteurs de la banque et de la distribution, présence croissante des grands distributeurs dans le domaine financier [(1)], développement des cartes co-marquées.

*(1) Tous les grands groupes de la distribution sont présents dans le secteur bancaire : Auchan, Carrefour, Casino, PPR, Nouvelles galeries, centres Leclerc, Intermarché, 3 Suisses…*

## 2.- Les cartes émises par des entreprises de droit commun

• **L'article 12-5° de la loi bancaire autorise une entreprise à émettre des cartes** délivrées pour l'achat auprès d'elle de biens ou services déterminés.

Les cartes émises par des entreprises non dotées du statut d'établissement de crédit sont donc, en principe, des cartes mono-prestataires qui se caractérisent par l'unicité de l'émetteur et du prestataire chez qui l'achat est réglé par carte.

Toutefois, selon le Comité des établissements de crédit et des entreprises d'investissement, cette « *disposition est interprétée de manière souple. Ainsi, l'émission de cartes que l'usage qualifie de privatives peut-elle être effectuée par une société pour l'achat de biens commercialisés aussi bien par elle-même que par des commerçants franchisés par elle* » (1).

De plus, en raison d'une interprétation bienveillante de l'article 12-5° par les pouvoirs publics, sont autorisées l'émission et la gestion d'une carte utilisable auprès de divers prestataires – carte dite multi-prestataires – dès lors que l'entité émettrice regroupe exclusivement les accepteurs de la carte et qu'une solidarité commerciale et financière a été organisée entre eux pour la sécurité des porteurs de la carte.

La combinaison des articles 12-1° et 12 -5° de la loi bancaire permet à une entreprise non dotée du statut d'établissement de crédit d'émettre et de gérer, non seulement une carte de paiement, mais aussi une carte de crédit pour faciliter l'achat de ses propres biens ou services. En revanche, le régime dérogatoire instauré par l'article 12 n'autorise pas une telle entreprise à délivrer une carte de retrait qui permettrait à son titulaire de retirer des espèces auprès de l'émetteur.

• **L'émission et la gestion d'une carte de fidélité** donnant droit à la délivrance d'un bien ou service, mais non d'une somme d'argent ne sont pas soumises aux dispositions de la loi bancaire.

Lorsque la carte de fidélisation permet d'utiliser les ristournes obtenues lors de l'achat de certains biens ou services pour le paiement d'autres prestations, elle doit être regardée comme une carte de paiement et est alors qualifiée de carte de fidélité-paiement. Elle entre alors dans le champ d'application de la loi bancaire, sauf bénéfice du régime dérogatoire de l'article 12-5°.

---

*(1) Voir le rapport 1998 du CECEI, pages 242 et suivantes.*

• **L'émission et la gestion de cartes-villes ou de monétique municipale**, permettant le règlement de services publics municipaux, sont des activités susceptibles d'être réalisées par le Trésor public, mais les fonds correspondants doivent être conservés par un comptable public et déposés au Trésor.

Par ailleurs, sont apparues des cartes-villes permettant le règlement des prestataires de services publics et des commerçants de la ville, notamment par imputation de ristournes consenties par ceux-ci. Dans une telle situation, la présence d'un établissement de crédit est impérative pour la gestion des fonds privés (le groupe Cofinoga est présent sur ce créneau).

Aucune donnée globale n'est disponible sur le nombre de cartes privatives émises et le volume des transactions effectuées grâce à leur utilisation. Les autorités de tutelle ont parfois connaissance de projets, car il leur est demandé s'ils sont compatibles avec les dispositions de la loi bancaire, mais l'activité menée étant par définition hors loi bancaire, aucun moyen d'investigation ne leur est conféré pour avoir des précisions chiffrées. On est en droit de penser, cependant, que le poids relatif des transactions opérées par carte privative demeure faible.

Au terme de cette analyse, un constat semble s'imposer : le domaine des cartes est en pleine évolution. Le cadre réglementaire, les acteurs, les produits, les comportements individuels sont en mutation. Encore, avons-nous, à dessein, limité notre investigation au territoire national. Or, plus que jamais, le secteur est directement influencé par le contexte international, qu'il soit d'ordre réglementaire ou technique. La multiplication des projets en matière de porte-monnaie virtuel et des problèmes posés par les paiements sur internet en est une illustration.

## C.- UN USAGE EN PROGRESSION CONSTANTE

### 1.- Des indicateurs en forte hausse

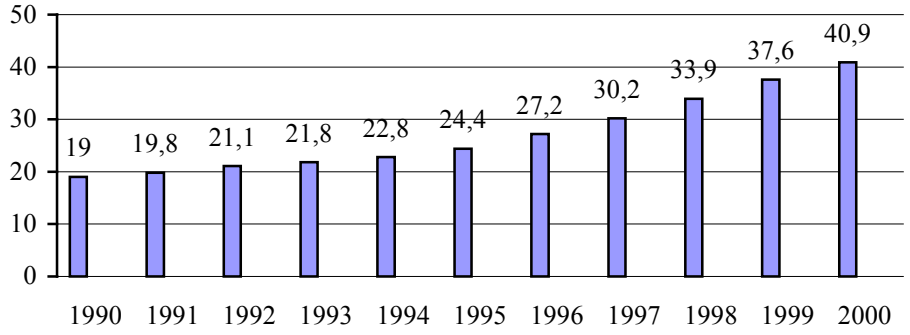
Tous les indicateurs traduisent un usage de plus en plus fréquent des cartes de paiement. Si l'on se limite aux cartes bancaires « CB », on constate les évolutions suivantes.

• **Nombre de cartes**

Le nombre de cartes bancaires « CB » est passé de 19 millions en 1990 à 40,9 millions en 2000. Entre 1998 et 1999, la progression de ce nombre a été de 11 % et, entre 1999 et 2000, de 9%.

**NOMBRE DE CARTES BANCAIRES « CB »**

*(en millions)*



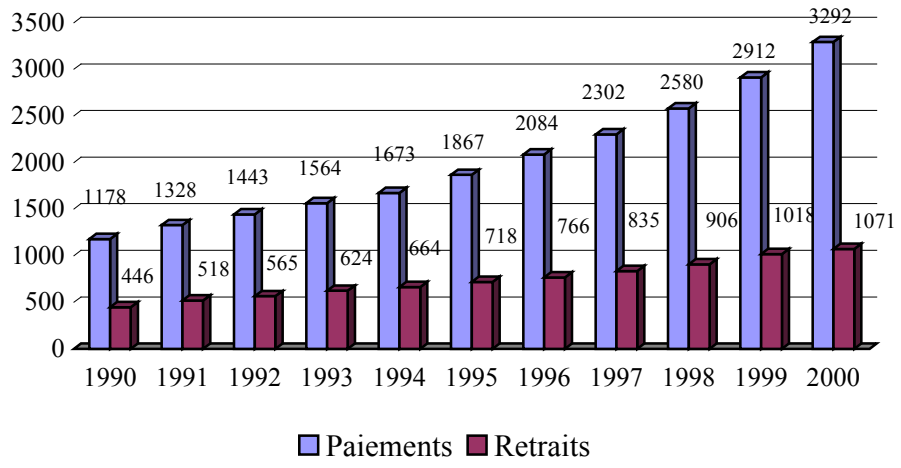

*Source : GIE cartes bancaires.*

- **Nombre de retraits et paiements**

Le graphique suivant illustre l'usage de plus en plus courant de la carte bancaire.

**NOMBRE DE RETRAITS ET DE PAIEMENTS PAR CARTES BANCAIRES « CB »**

*(en millions)*



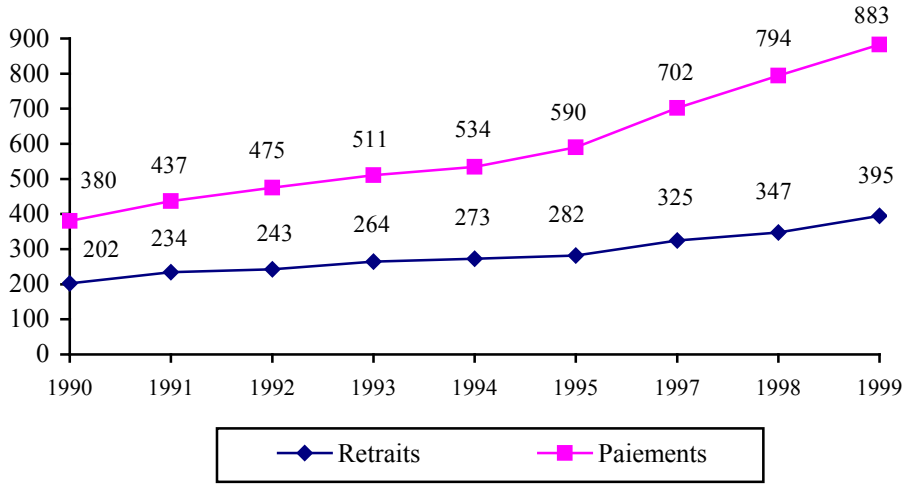

*Source : GIE cartes bancaires.*

• **Montant des paiements et des retraits**

Les 2,912 milliards d'achats réalisés en 1999 avec une carte bancaire « CB » ont représenté 883 milliards de francs. Par ailleurs, les 1,018 milliard de retraits ont concerné 395 milliards de francs. Le volume d'activités de 1999 s'est donc élevé à 1.278 milliards de francs (soit 194,83 milliards d'euros et ce chiffre a atteint 217,03 milliards d'euros en 2000), contre 582 milliards de francs en 1990.

**MONTANT DES PAIEMENTS ET DES RETRAITS PAR CARTES BANCAIRES « CB »**

*(en milliards de francs)*

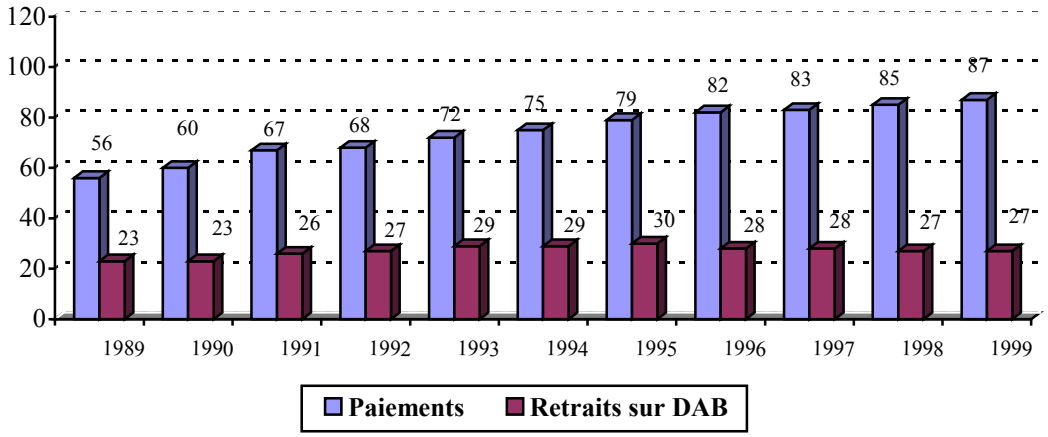



*Source : GIE cartes bancaires.*

• **Nombre de transactions par carte et par an**

Avec une moyenne de 114 opérations par carte et par an, en 1999, les cartes « CB » sont les cartes les plus utilisées dans le monde.

**NOMBRE DE TRANSACTIONS PAR CARTE « CB »
ET PAR AN**




*Source : GIE cartes bancaires.*

- **Nombre des dispositifs d'acceptation**

Cette importante utilisation de la carte bancaire « CB » est rendue possible par l'augmentation parallèle du nombre des dispositifs d'acceptation.

Ainsi, pour les paiements, 623.000 commerçants, prestataires de service ou administrations, acceptaient la carte bancaire en 1999.

**DISPOSITIFS D'ACCEPTATION POUR LES PAIEMENTS
en 2000**

| | |
|---|---|
| Terminaux de paiement électronique indépendants | 610.000 |
| Systèmes intégrés | 130.000 |
| Automates | 27.000 |
| Publiphones acceptant les cartes à puce | 210.000 |
| Imprimantes manuelles | 35.000 |
| Minitels de type Magis | 600.000 |
| Lecteurs sécurisés Internet | 20.000 |
| Décodeurs Canal + équipés d'un lecteur carte à puce | 1.700.000 |
| Téléphones mobiles | 200.000 |
| **TOTAL** | **3.567.160** |

*Source : GIE cartes bancaires.*

On peut ainsi noter qu'il y avait 610.000 terminaux de paiement électroniques (TPE), en 2000, contre 65.000 en 1986.

S'agissant des retraits, le nombre des DAB, qui était de 10.000 en 1988, s'élevait à 35.160 en 2000.

Le succès de la carte bancaire « CB » est lié à la satisfaction que les utilisateurs en retirent. Ainsi, selon une étude réalisée par la SOFRES, du 6 au 12 juillet 2000 auprès de 805 porteurs de cartes bancaires, 95% des personnes interrogées se déclarent satisfaites de l'utilisation de leur carte pour régler leurs achats et 98% ont une opinion identique pour le retrait des espèces. De même, selon une étude effectuée par le même organisme, du 8 au 17 octobre 1998, auprès de 800 responsables de magasins, 95% des commerçants sont satisfaits du système « CB ».

Enfin, il importe d'observer que le 23 décembre 2000 – c'est-à-dire à une période où le problème de la sécurité des cartes bancaires était fréquemment évoqué par la presse – tous les records du nombre d'autorisations ont été battus : 6,4 millions d'autorisations ont transité dans le réseau, ce qui représente entre 30 et 35 millions de paiements par carte pour cette seule journée.

## 2.- Une croissance réalisée aux dépens du chèque

La carte, conçue à l'origine pour réduire le nombre de chèques émis a rempli cet objectif, même si le chèque demeure le mode de paiement préféré de nos concitoyens.

**INSTRUMENTS DE PAIEMENT ECHANGES DANS LES SYSTEMES DE PAIEMENT**

*(en milliers d'opérations)*

| | **1995** | **1996** | **1997** | **1998** | **1999** |
|---|---|---|---|---|---|
| Chèques | 3.8 | 3.9 | 3.9 | 3.8 | 3.6 |
| Virements | 1.1 | 1.1 | 1.2 | 1.3 | 1.3 |
| Lettres de change relevées | 129.2 | 129.2 | 124.8 | 125.2 | 121.2 |
| Avis de prélèvement | 850.2 | 927.5 | 987.1 | 1.0 | 1.2 |
| TIP | 91.0 | 114.3 | 122.3 | 129.4 | 131.6 |
| Télépaiements | 195 | 193 | 230 | 299 | 415 |
| **Paiements par carte** | **1.8** | **1.8** | **1.9** | **2.1** | **2.4** |
| Retraits aux DAB et GAB | 443.9 | 482.5 | 520.2 | 569.3 | 614.5 |
| **Total** | **8.3** | **8.6** | **8.8** | **9.3** | **9.6** |

*Source : Banque de France.*

On peut dès lors observer que les chèques, qui représentaient 47% des instruments de paiement échangés dans les systèmes de paiement en

1995, ont vu cette part réduite à 39% en 1999. Dans le même temps, la part des paiements par carte est passée de 22% à 26%.

Pour conforter cette évolution, il importe que les consommateurs aient confiance dans cet instrument de paiement. Or, une réticence est manifeste en ce qui concerne les paiements en ligne par carte bancaire. Le récent rapport réalisé dans le cadre du Conseil national de la consommation observe que le volume des paiements en ligne à l'aide de la carte bancaire serait de l'ordre de 0,15% du volume des achats du commerce de détail et que le paiement à distance par carte « CB » représenterait seulement 3,5% des paiements effectués à l'aide de cet instrument de paiement. Redonner confiance aux consommateurs est donc essentiel pour le développement du commerce électronique et pour soutenir l'industrie française de la puce.

## II.- UN SECTEUR DE POINTE DE L'INDUSTRIE FRANÇAISE

Dans la préface qu'il a rédigée pour un « Que sais-je ? » récent [(1)], Roland Moreno, l'homme qui a déposé le brevet de la carte à puce, fait état de deux chiffres dont le rapprochement est impressionnant : l'Etat n'aurait misé que 250.000 francs sur ce brevet, qui aurait déjà généré un milliard de francs de royalties.

L'invention de la carte à puce a effectivement permis, en France, le développement d'une véritable industrie de la monétique, nécessitant de nombreux savoir-faire.

Il faut en effet :

– fabriquer les supports de cartes,

– les équiper de microcircuits,

– les personnaliser,

– fabriquer les terminaux de paiement, les automates bancaires,

– développer les logiciels qui les équiperont,

– enfin, assurer une logistique informatique pour les circuits d'échanges, d'autorisation, de compensation.

Les principales entreprises intervenant dans ce secteur sont :

---

*(1) Jean Donio, Jean Leroux les Jardins, Edouard de Rocca et Malika Verstrepen, «* La carte à puce *», 1999.*

– pour les supports : Gemplus, Oberthur CS, Ruwaplast, Sagem et Schlumberger ;

– pour les composants des puces équipant les cartes « CB » : ST Microelectronics… ;

– pour les encarteurs : Gemplus, Oberthur CS, Sagem et Schlumberger ;

- pour les personnalisateurs : Cedicam, CPS Technologies, Gemplus, Oberthur CS, Schlumberger et Sibe ;

– pour les terminaux de paiement agréés « CB » : Ascom Monetel, CEICOM, CKD Moneyline, Dassault AT, Ingenico, Sagem, Schlumberger et Verifone ;

– pour les distributeurs automatiques de billets : Bull, Dassault A.T., Nixdorf, Diebold, Getronics et NCR.

Actuellement, on peut estimer que l'offre de cartes bancaires est à 90% européenne et aux deux tiers française.

La société française Gemplus est, avec 43% du marché mondial, le principal encarteur. Son chiffre d'affaires s'est élevé à 5.029 milliards de francs en 1999 et elle employait, en juin 2000, 7.000 salariés répartis dans plus de 30 pays, mais dont la moitié travaillent en France.

Le marché de la carte bancaire est en croissance de 30 à 40% chaque année [(1)] et les prévisions à court terme prévoient la poursuite de cette évolution.

*(1) Roland Moreno, «* Théorie du Bordel ambiant *», p. 348, 2000.*

**PREVISIONS DU MARCHE DE LA CARTE A PUCE**

*(en millions)*

| Marché | 1997 | 2003 | Croissance annuelle |
|---|---|---|---|
| Télécartes | 684 | 3.270 | 30% |
| GSM | 69 | 760 | 49% |
| **Banque** | **49** | **690** | **55%** |
| Fidélité | 22 | 320 | 56% |
| Santé | 16 | 210 | 54% |
| TV à péage | 12 | 150 | 52% |
| Transport | 8 | 240 | 77% |
| Jeux | 2 | 70 | 78% |
| Contrôle d'accès | 10 | 260 | 72% |
| Identité | 2 | 50 | 71% |
| Technologie de l'information | 1 | 120 | 142% |
| Autres | 24 | 170 | 30% |
| **TOTAL** | **900** | **6.310** | **38%** |

*Source : Gemplus, cité dans « La carte à puce », Que sais-je n° 3492.*

Le tableau précédent montre clairement que la télécarte représente la principale production (80% de la production totale actuelle de cartes à puce), très loin devant la carte bancaire. Mais, pour l'avenir, la banque représente, derrière la téléphonie mobile, le deuxième grand gisement de volume.

Le futur de la carte à puce passe également par les domaines de la santé (Sesam vitale, par exemple), des transports publics ou de l'identité.

Ces perspectives de développement ne doivent pas être remises en cause par des craintes disproportionnées concernant la sécurité de la carte à puce.

## CHAPITRE II

## UNE SECURITE POTENTIELLEMENT FORTE

L'absolue nécessité de la sécurisation des cartes bancaires constitue une évidence. Qu'en est-il pourtant aujourd'hui dans les faits ?

Toutes les statistiques – même celles fournies par le Groupement des cartes bancaires – traduisent une progression de la fraude. Toutefois, l'étude de la typologie de cette fraude conduit à relativiser son importance et, en tout état de cause, incite à proscrire les propos exagérément alarmistes.

### I.- UNE FRAUDE EN PROGRESSION

Depuis 1999, les données chiffrées sur la fraude, communiquées par le Groupement des cartes bancaires, montrent que la fraude, en diminution constante jusqu'alors, amorce une remontée. Ces chiffres « officiels » ne reflètent que partiellement la situation réelle, dans la mesure où la définition de la fraude retenue par le Groupement est singulièrement restreinte et ne tient pas compte des multiples facettes de cette délinquance.

#### A.- LES DONNEES FOURNIES PAR LE GROUPEMENT DES CARTES BANCAIRES

Les seules statistiques « officielles » disponibles sont celles fournies par le Groupement des cartes bancaires. Les pouvoirs publics ne disposent pas, en effet, d'autres sources d'information sur le volume de la fraude. Les seuls éléments susceptibles d'apporter un éclairage complémentaire sont les renseignements statistiques recueillis par les services de la police nationale et des unités de la gendarmerie nationale, qui indiquent qu'entre 1999 et 2000, les infractions relatives aux cartes de crédit ont augmenté de 25,23%.

**MONTANT ET TAUX DE LA FRAUDE**

*(en millions de francs)*

| | En France sur cartes « CB » | | | | « Hors frontières » | | | |
|---|---|---|---|---|---|---|---|---|
| | Paiements | | Retraits DAB | | Paiements par cartes « CB » à l'étranger | | Paiements par cartes étrangères en France | |
| | Montant | Taux (en %) | Montant | Taux (en %) | Montant | Taux (en %) | Montant | Taux (en %) |
| 1995 | 160 | 0,028 | - | - | - | - | - | - |
| 1999 | 178 | 0,020 | 61 | 0,015 | 141 | 0,47 | 220 | 0,49 |
| 2000 | 250 | 0,026 | 70 | 0,017 | 195 | 0,57 | 340 | 0,53 |

*Source : GIE cartes bancaires.*

Le taux global de la fraude (paiements et retraits), en 2000, dans le système « CB » en France, s'élève à 0,023% contre 0,018% en 1999. Par ailleurs, pour les six premiers mois de l'année 2000, le taux de fraude des opérations à distance se monte à 0,11%, dont la moitié résulte des problèmes liés aux rechargements à distance des cartes de téléphonie mobile prépayées (le taux de fraude dans ce secteur atteignant 1,2%).

De ces chiffres, plusieurs constatations peuvent être tirées.

**– Une hausse sensible de la fraude sur l'ensemble des opérations.**

Entre 1999 et 2000, le volume des paiements frauduleux a augmenté de 40% et le volume des retraits frauduleux de 14%.

Plus encore, le montant des paiements frauduleux par cartes « CB » à l'étranger a progressé de 38%, tandis que les paiements frauduleux par cartes étrangères en France ont connu une croissance de 54%.

**– Des taux de fraude sensiblement différents, selon les conditions d'utilisation de la carte bancaire.**

Le taux de fraude varie de 0,017% (pour les retraits en France) à 0,57% (pour les paiements par cartes « CB » à l'étranger), soit un rapport de 1 à 33.

**– Un risque accru à l'étranger et pour les transactions effectuées avec des cartes étrangères.**

Les chiffres fournis par le GIE cartes bancaires montrent clairement que le risque d'être victime d'une fraude est sensiblement accru, lorsque les porteurs font usage de leur carte à l'étranger, ce qui correspond toutefois à une situation peu fréquente, puisque 98% des transactions par cartes « CB » se réalisent en France. Il convient d'ailleurs de réaffirmer ici l'avertissement formulé par le rapport réalisé dans le cadre du Conseil national de la consommation : « *Il ne faut évidemment* ***jamais*** *composer son code secret dans un pays étranger pour le paiement à proximité* », dans la mesure où les risques de fraude à la « *white plastic* » seraient ainsi accrus.

En outre, il apparaît nettement que les commerçants sont totalement exposés au risque de fraude lorsqu'une carte étrangère est utilisée pour réaliser des paiements. On peut constater, en effet, que le montant des opérations frauduleuses dans cette hypothèse (340 millions de francs en 2000) est très supérieur à celui concernant les paiements opérés avec une carte « CB » (250 millions de francs).

## B.- UNE APPROCHE PARTIELLE ET RESTRICTIVE DE LA FRAUDE

Les chiffres cités précédemment sont loin de prendre en compte l'intégralité du phénomène de la fraude car, d'une part, ils ignorent la fraude sur les cartes privatives et, d'autre part, la définition de la fraude retenue par le Groupement des cartes bancaires conduit à ne faire apparaître que la fraude déclarée par les banques. Comme le souligne le rapport réalisé dans le cadre du Conseil national de la consommation, il est donc « *impossible de disposer d'une évaluation quantitative globale de la fraude en France* ».

### 1.- Une relative inconnue la fraude sur les cartes privatives

Les émetteurs de cartes privatives ne communiquent guère sur les taux de fraude qu'ils enregistrent. Le rapport du groupe technique restreint mis en place au sein de la mission « commerce électronique » du ministère de l'économie, des finances et de l'industrie, constate même que « *les émetteurs* Diners *et* American express *n'ont pas jugé opportun de communiquer d'informations à ce sujet* ».

Certaines informations ont néanmoins été transmises lors des auditions réalisées par le groupe de travail chargé d'effectuer un rapport dans le cadre du Conseil national de la consommation.

Cetelem a ainsi indiqué que son taux de fraude se monte à 0,05% pour les paiements et les retraits de proximité (en montant). De son côté, Cofinoga a fait savoir que le taux de fraude est de 0,01% du chiffre d'affaires dans les hypermarchés où le code secret est utilisé et de 0,07% du chiffre d'affaires dans les grands magasins où le code secret n'est pas demandé. *American express* a donné un taux de fraude de 0,07% pour l'ensemble des transactions faites en France et à l'étranger, que celles-ci soient des paiements à distance ou des paiements de proximité.

Ces indications demeurent lacunaires, mais un fait est néanmoins frappant : les taux de fraude fournis par ces émetteurs sont sensiblement supérieurs à ceux du GIE cartes bancaires pour les paiements de proximité effectués en France. Cela ne peut que renforcer les doutes sur la pertinence des chiffres communiqués par ce Groupement.

### 2.- Une vision strictement bancaire de la fraude

Aux termes d'une réponse faite par le Groupement des cartes bancaires à votre Rapporteur pour avis, les chiffres de la fraude « *résultent d'une agrégation des déclarations de fraude fournies par toutes les banques « CB » au système d'information du GIE (SICB). Dès lors qu'une fraude (utilisation illégitime de la carte ou de son numéro) est portée à la connaissance de la banque (ou détectée par elle), celle-ci est déclarée par la banque émettrice de la carte via un échange informatique au SICB. La fiabilité des chiffres du « GIE » est donc le reflet exact de celle des déclarations des banques « CB », dont les montants figurent en perte à leur compte d'exploitation. Le processus est identique pour les déclarations de fraude intervenant à l'étranger, étant précisé que ce sont les réseaux internationaux Visa et MasterCard qui nous fournissent les chiffres, puisqu'il s'agit de fraudes réalisées avec des cartes CB (Visa ou MasterCard) chez des commerçants à l'étranger et dont la comptabilisation est assurée par les banques de ces commerçants puis déclarée à Visa et MasterCard* ».

Les données communiquées par le GIE ne prennent donc en compte que la fraude supportée par les banques [(1)], ce qui signifie que la définition de la fraude retenue par cet organisme écarte :

– les fraudes antérieures aux déclarations de vols et de pertes (c'est-à-dire celles antérieures à la mise en opposition). Or, il est probable que cette fraude non recensée est supérieure à la fraude postérieure à la mise

*(1) Il semblerait, par ailleurs, que les données transmises par les banques mutualistes au GIE concernent une fraude dont la définition est encore plus restrictive que celle retenue par le Groupement.*

en opposition. Dans le cas du vol d'une carte, en particulier, il est évident que les fraudeurs agissent au plus vite, avant que la victime ait le temps de s'apercevoir de la disparition de la carte ;

– les fraudes résultant d'opérations à distance laissées à la charge des commerçants : il convient effectivement de préciser qu'en application des articles 1315 et suivants du code civil, relatifs à la preuve des obligations et des paiements, les commerçants intervenant dans le domaine de la vente à distance autorisent expressément, dans le contrat de vente spécifique aux opérations de vente à distance, leur banque à débiter d'office leur compte du montant de toute opération réalisée sans usage du code secret permettant d'authentifier le porteur, dont la réalité serait contestée par écrit par le titulaire de la carte ;

– d'une façon plus générale, probablement, les fraudes liées à l'utilisation frauduleuse des cartes et, en particulier, les affaires dites de « *white plastic* » où les fraudeurs copient la piste magnétique d'une carte sur un support vierge (en général blanc, d'où le nom de « *white plastic* »), puis retirent de l'argent sur le compte de la victime en usant de son code confidentiel qu'ils ont préalablement obtenu (soit en épiant un retrait effectué par le porteur, soit par des moyens techniques plus complexes visant à pirater le code lorsqu'il est composé sur un clavier de TPE). Dans cette hypothèse où le code secret – également appelé « code PIN » (« *Personal Identification Number* ») – est mis en œuvre, les banques ont tendance à ne pas recréditer le porteur, qui s'est engagé par contrat à ne jamais dévoiler son code à un tiers.

Dès lors, le taux global de la fraude dans le système « CB » en France est certainement supérieur au taux de 0,023% annoncé pour 2000, correspondant à un montant de 320 millions de francs.

L'importance réelle de la fraude est cependant difficile à évaluer en l'absence d'outils statistiques pertinents. On peut simplement signaler les estimations effectuées par des associations de consommateurs, en fonction des réclamations reçues.

Ainsi, l'Association française des usagers des banques (AFUB) chiffre à 1,6 milliard de francs la fraude totale en 1999 (alors que le GIE cartes bancaires ne reconnaît, pour la même année, qu'un montant de 600 millions de francs). Plus encore, l'association Force ouvrière consommateur considère que ce montant total est de 3 milliards de francs, et que le GIE sous-évalue, en particulier, la fraude sur les paiements en France avec une carte « CB » (890 millions de francs au lieu de 178 millions de francs) et avec une carte étrangère (1.950 millions de francs, contre 200 millions de francs admis par le GIE).

Aucun élément ne permet à votre Rapporteur pour avis de trancher entre toutes ces données chiffrées, mais – au-delà des données brutes – il importe d'examiner précisément les fraudes mises en œuvre, ce qui conduit à en dresser une typologie.

## II.- UNE FRAUDE TRES DIVERSIFIEE

Plusieurs approches typologiques sont envisageables. La plus fréquemment retenue, celle qui est utilisée notamment pour présenter les statistiques de la fraude, pourrait être qualifiée de « consumériste », dans la mesure où elle permet d'informer les consommateurs sur les situations d'utilisation de la carte les plus risquées. Il convient, néanmoins, de compléter ce point de vue par une perspective technique, mettant en exergue les dispositifs de sécurité contournés par les fraudeurs, ainsi que par une approche « répressive » étudiant le niveau d'organisation de la criminalité en cause.

### A.- UNE APPROCHE CONSUMERISTE

Dans ce cas de figure, la fraude est classée en fonction des usages de la carte.

#### 1.- La fraude dans le paiement en face à face

– La principale fraude est l'utilisation d'une carte authentique volée par un malfaiteur ayant réussi à se procurer le code secret.

Il est intéressant d'observer que, lors de leur audition par le groupe travaillant au sein du Conseil national de la consommation, deux émetteurs de cartes privatives (Cetelem et Cofinoga) ont insisté sur le fait que le vol avait lieu essentiellement (98% des cas, selon Cetelem), dans les circuits postaux. Cofinoga a même précisé que les services de filiales de La Poste sont utilisés pour éviter que l'envoi passe par certains « *centres de tri postaux davantage exposés* ».

– Une fraude, en voie de disparition, est celle de type « rejeu », c'est-à-dire un deuxième paiement effectué par le commerçant. Cette fraude était facile avec les terminaux de paiement de l'ancienne génération (« fers à repasser »), mais elle devient impossible avec les TPE. Elle perdure néanmoins à l'étranger et est d'ailleurs souvent qualifiée de « fraude à la thaïlandaise ».

## 2.- La fraude lors de retraits aux DAB

Le rapport du groupe technique restreint travaillant au sein de la mission « commerce électronique » du ministère de l'économie, des finances et de l'industrie estime que cette fraude peut être classée en quatre catégories :

– la violence à l'encontre du possesseur de la carte, qui permet de s'emparer non seulement des espèces retirées par ce dernier, mais également de sa carte et de son code secret ;

– l'abus de confiance – également qualifié par l'une des personnes auditionnées par votre Rapporteur pour avis de « délinquance du strabisme divergent » - qui consiste à observer le code composé et à subtiliser la carte (à un moment, qui peut être ultérieur, ce qui est plus simple à pratiquer avec une personne de son entourage) ;

– l'exploitation de failles dans l'organisation : diverses méthodes sont envisageables, telle que la complicité avec un employé chargé d'opérations sur le distributeur ou la modification superficielle de l'appareil. On rencontre, notamment ici, la désormais célèbre technique du « collet marseillais », qui consiste à mettre un élément étranger au fond du lecteur de carte du DAB pour bloquer la carte introduite, puis à la récupérer pendant que son porteur légitime s'est éloigné, croyant que sa carte avait été avalée par le distributeur ;

– l'utilisation d'informations collectées en paiement en face à face. Cette fraude, apparemment en fort développement (elle aurait concerné 3.000 personnes en 2000), implique de copier la piste magnétique d'une carte (technique dite du « *skimming* »), généralement grâce à un commerçant indélicat dont le TPE est modifié, et de la dupliquer ultérieurement, soit sur un support vierge (la « *white plastic* » déjà évoqué précédemment), ne posant aucune difficulté d'utilisation sur les DAB, soit sur une carte ayant l'apparence d'une véritable carte bancaire, lorsqu'il s'agit de tromper un commerçant dans le cadre d'un paiement en face à face. Cette méthode frauduleuse nécessite également la connaissance du code secret, mais elle peut être acquise également grâce à une manipulation sur le TPE du commerçant complice. A titre d'exemple, la police d'Aubervilliers a arrêté, fin août 2000, un pompiste ayant ainsi recueilli les données essentielles des cartes bancaires d'environ 400 personnes.

### 3.- La fraude avec des cartes étrangères utilisées en France

Les commerçants français sont exposés à deux risques principaux :

– l'utilisation d'une carte contrefaite : la technique du « *skimming* » précédemment décrite s'avère difficile à contrer lorsque les pistes copiées (qui peuvent être celles de véritables cartes émises en France), sont produites sur des cartes censées avoir été émises à l'étranger, dont les commerçants français n'ont qu'une faible connaissance, compte tenu des très nombreux visuels en circulation dans le monde ;

– l'utilisation d'une véritable carte : la révocation de l'achat est une possibilité légale, largement utilisée dans d'autres pays, et notamment en Amérique du Nord. Ce risque est aggravé par la distance, qui rend impraticable une poursuite judiciaire de clients étrangers pour des montants faibles.

### 4.- La fraude sur les paiements à distance

La vente à distance englobe évidemment le commerce électronique, dont le développement constitue pour beaucoup l'un des enjeux économiques de ces prochaines années. Mais la vente à distance ne se résume pas au commerce électronique. La « traditionnelle » vente par correspondance, les commandes par téléphone et – il ne faut pas l'oublier – par Minitel, représentent encore l'essentiel du chiffre d'affaires de ce secteur (selon la Fédération des entreprises de vente à distance, le Minitel génère 6 milliards de francs du chiffre d'affaires de la vente à distance, contre 2 milliards de francs pour Internet)

Si le commerce électronique n'est pas toute la vente à distance, il serait de même illusoire de penser que la carte bancaire est le seul moyen de paiement envisageable, voire souhaitable, pour les achats sur Internet.

En matière de paiements à distance, les risques d'un achat non sécurisé sont divers :

– le numéro de la carte peut être piraté pour être utilisé à des fins frauduleuses : ce piratage peut revêtir des formes plus ou moins complexes.

Les plus simples consistent à relever ces données sur la carte d'un proche ou sur les facturettes les mentionnant encore.

Mais il existe des variantes plus technologiques, qui seront examinées ci-après ;

– le montant de l'achat peut être modifié par un commerçant malhonnête ;

– le site sur lequel la commande est réalisée peut ne pas être le site officiel du commerçant avec lequel le consommateur croit traiter ;

– le porteur de la carte peut contester à tort l'achat qu'il a effectué.

Dans le domaine de la vente à distance, il importe de distinguer le secteur traditionnel de celui de la téléphonie mobile. Ce dernier secteur a enregistré une hausse importante de la fraude dans les premiers mois de 2000 sur les paiements des rechargements des cartes prépayées. En revanche, le secteur traditionnel est beaucoup moins exposé (notamment du fait des mesures de précaution prises par les entreprises de vente par correspondance), à l'exception, semble-t-il, d'activités moins sécurisées (joaillerie, voyages, informatique).

### B.- UNE APPROCHE TECHNIQUE

La classification « consumériste » a le mérite d'alerter les porteurs de cartes sur les situations où leur vigilance doit être renforcée, mais il convient de la compléter par une étude des éléments de sécurisation contournés par les fraudeurs pour mieux évaluer les risques pesant sur l'usage de la carte bancaire.

La sécurité de la carte bancaire repose sur trois éléments principaux :

– les données visibles sur la carte en plastique (numéro à seize chiffres, nom du porteur, date d'expiration, hologramme, et, le cas échéant, cryptogramme visuel figurant au dos de la carte) ;

– les informations enregistrées sur la piste magnétique ;

– les données stockées dans la puce.

Il importe, par ailleurs, de ne pas oublier que les terminaux (TPE, DAB…) constituent des maillons importants de la chaîne sécuritaire.

### 1.- Les données visibles sur la carte plastique

Une carte bancaire est, à première vue, un simple rectangle de plastique de format 85,6 x 54 mm. Elle est conforme à une norme ISO (*International Organisation for Standardization*).

Elle comporte une signalétique qui identifie l'émetteur et le réseau auquel elle appartient, ainsi qu'un hologramme. En outre, sont embossés [(1)]le numéro à seize chiffres, le nom du porteur et la date de validité de la carte. Au verso, se trouvent un exemplaire de la signature du titulaire et, sur certaines cartes, un cryptogramme visuel de trois chiffres (qui dans le jargon fort usité de ce milieu porte le nom de CVV 2 pour le réseau Visa, de CVC 2 pour le réseau MasterCard et de CVN 2 pour les cartes nationales).

Comme l'observe le rapport précité du groupe technique restreint, « *le numéro de carte, le nom du porteur et la date de validité ne sont nullement sécurisés, de même que la signature du porteur* ». Il existe, en effet, de nombreuses façons, très simples pour se procurer ces données.

Tout d'abord, elles sont parfois transmises directement par le porteur de la carte, notamment pour effectuer des réservations dans les hôtels ou auprès des loueurs de voiture. Il importe pourtant de reproduire ici une réponse faite par le Groupement des cartes bancaires à votre Rapporteur pour avis :

« *Il n'existe pas d'obligation pour qui que ce soit de donner une numéro de carte pour réserver une nuitée dans un hôtel. Si une telle obligation existe, elle serait le fait du commerçant qui n'a pas en principe de raisons commerciales d'imposer à son client son choix de moyen de paiement. En toutes hypothèses, dans les règles interbancaires « CB », c'est-à-dire celles qui lient les banques membres du Groupement et s'imposent à elles, il est interdit d'utiliser la carte « CB » comme un instrument permettant de constituer une caution. Cette caution serait illicite car son débiteur serait la banque du porteur, qui a émis la carte et qui n'a jamais donné son consentement pour servir de caution* ».

La plupart du temps, néanmoins, les fraudeurs se procurent les données embossées sur la carte à l'insu du porteur. Dans certains cas, ce sont des proches (membres de la famille, collègues…), mais plusieurs possibilités permettent à des fraudeurs de se procurer ces informations sans appartenir à l'entourage du porteur.

---

*(1) L'embossage est un procédé d'écriture sur une carte plastique faisant apparaître les caractères en relief.*

Ils peuvent, en premier lieu, les relever sur les facturettes émises par des TPE ne tronquant pas ces informations.

Des variantes plus sophistiquées existent également :

– construction de numéros de carte cohérents à partir des règles qui régissent leur syntaxe ;

– utilisation des sites Internet dits de « *carding* », diffusant des numéros de cartes valides. Le Conseil de sécurité intérieure du 30 janvier 2001 recensait 250 sites générateurs de numéros de carte, dont trois installés en France.

Ces deux techniques sont, toutefois, de faible rendement car l'utilisation d'une carte impose de disposer également du nom du porteur et de la date de validité ;

– intrusion informatique dans les bases d'entreprises stockant les données concernant leurs clients. De nombreuses affaires ont été révélées récemment. Ainsi, début septembre 2000, 15.700 numéros de cartes ont été volés sur le site de *Western Union Financial Services Corp*. En mars 2001, *Bibliofind*, une filiale d'*Amazon*, admettait que 98.000 fiches de clients avaient été dérobées ;

– capture du numéro lors de la transmission sur le réseau Internet, lorsque celle-ci n'est pas suffisamment sécurisée.

Il apparaît donc relativement aisé pour les fraudeurs de s'emparer des données figurant en clair sur l'ensemble des cartes. Il convient, néanmoins, de ne pas surestimer les risques encourus du fait de ce type de fraude car :

– elle ne peut trouver à s'appliquer que dans le cadre de la vente à distance (et, en aucun cas, pour les paiements en face à face ou les retraits aux DAB) ;

– dès lors, la victime de la fraude dont le code secret n'a pas, par définition, été composé lors de l'achat frauduleux, peut exiger la recréditation de son compte par sa banque (application des articles 1315 et suivants du code civil précités, dont les dispositions sont rappelées par le contrat spécifique de la vente à distance) ;

– différents moyens techniques existent pour réduire l'importance de cette fraude : modification des TPE, afin que les facturettes émises ne comportent plus les données complètes ; protection accrue des banques de

données conservées par les entreprises se livrant au commerce électronique ; généralisation du cryptogramme visuel de trois chiffres au verso rendant impossible l'utilisation d'une carte sans être en sa possession (ou du moins sans l'avoir eu temporairement en sa possession) puisque ce numéro serait demandé systématiquement par le commerçant lors de la commande ; sécurisation des transmissions par des outils tels que les protocoles SSL (*Secure Socket Layer*) (1) ou SET (*Secure Electronic Transaction*) (2) avec, le cas échéant, une précaution supplémentaire consistant à utiliser un lecteur connecté à son ordinateur, afin que seules les informations concernant le paiement (montant et compte à débiter) soient transmises sur le réseau sécurisé (c'est le principe du boîtier Cyber-comm développé par le Groupement des cartes bancaires) . De multiples autres solutions techniques existent, de la carte virtuelle dynamique visant à générer des numéros de carte spécifiques à chaque transaction et donc non réutilisables à des initiatives tendant à l'utilisation d'une carte à puce dédiée à Internet (« chéquier électronique », …) qui ne serait donc plus, à proprement parler une carte bancaire. Votre Rapporteur pour avis reviendra sur ces différents procédés dans la suite du présent rapport et dans son futur rapport d'information.

### 2.- Les informations enregistrées sur la piste magnétique

La piste contient les informations figurant en clair sur la carte (le numéro à seize chiffres, la date de validité et le nom du porteur) et quelques informations complémentaires d'authentification.

Il s'agit de la méthode de sécurisation la plus usitée hors de France et en matière de cartes privatives. Le porteur de la carte est, en outre, identifié, soit par la frappe d'un code secret à quatre chiffres (ce qui est le cas en France pour les cartes « CB » ou les cartes Cofinoga dans certaines enseignes les acceptant), soit par la signature de la facturette.

Ce système de sécurisation présente néanmoins des garanties assez faibles.

D'une part, la copie des informations contenues dans une piste magnétique semble désormais assez aisée à réaliser (3) (technique du « *skimming* » précédemment décrite, permettant la réalisation de « *white*

---

*(1) Il s'agit d'un protocole de communication permettant l'établissement d'un canal de confidentialité pour la transmission du numéro de carte bancaire de l'acheteur vers le commerçant.*

*(2) Ce protocole développé par Visa et Mastercard permet, en outre, l'identification des acteurs du paiement.*

*(3) La copie d'une piste peut être effectuée en deux secondes.*

*plastic* » ou de cartes pourvues d'un visuel, souvent celui d'un pays étranger, du moins à première vue).

D'autre part, la sécurité du code à quatre chiffres se situe à un faible niveau puisque, même si le fraudeur n'a pu se le procurer grâce à la négligence du porteur ou du défaut de cache sur les boîtiers, cette protection n'est guère difficile à « casser » : il n'y a que 9999 combinaisons différentes (ce qui implique que 3.800 cartes environ utilisent le même code en France [(1)]). En outre, comme cela a déjà été indiqué, des TPE trafiqués permettent d'enregistrer le code secret.

Les fraudeurs munis de ces deux éléments (la copie de la piste magnétique et le code PIN) sont en mesure d'effectuer des paiements en face à face et des retraits sur les DAB dans tous les cas où la puce n'est pas mise en œuvre, à savoir :

– les paiements en face à face sur les terminaux de paiement ne demandant pas une autorisation systématique des opérations à la banque, c'est-à-dire les terminaux mécaniques (les « fers à repasser ») et les TPE lorsque le montant ne dépasse pas un seuil négocié entre le commerce et sa banque (généralement 600 francs [(2) (3)]) ; les cartes « CB » fonctionnant, en effet, en mode « semi *off-line* » ;

– les retraits effectués sur des DAB non équipés pour traiter la puce (33% des DAB au 1er janvier 2001 selon le Groupement des cartes bancaires [(4)]) ;

– les opérations réalisées à l'étranger, car les terminaux de paiement et les DAB n'y lisent que la piste magnétique. S'agissant des paiements, toutefois, il importe de noter que sur les TPE fonctionnant à l'étranger, une vérification « *on line* » est systématiquement pratiquée

---

*(1) Pour autant, personne ne préconise un rallongement de ce code, puisqu'un code à six chiffres, par exemple, ne serait pas excessivement plus difficile à casser et poserait des problèmes de mémorisation, ce qui, en fin de compte, serait susceptible de réduire sa confidentialité.*

*(2) Le seuil est susceptible d'être abaissé pour les commerces exerçant dans un secteur d'activité à risque.*

*(3) Pour les montants inférieurs à ce seuil, des demandes d'autorisation peuvent être faites de façon aléatoire par le TPE.*

*(4) Les DAB équipés pour lire la puce doivent néanmoins continuer à accepter les cartes à piste d'origine étrangère non munies de puce ainsi que les cartes de retrait munies uniquement d'une piste magnétique. Les risques de «* white plastic *» ne sont donc pas totalement écartés par la généralisation des DAB lecteurs de puce. En revanche, s'agissant d'une carte de paiement émise en France, les DAB équipés ne peuvent lire que la puce : la lecture des quatre premiers chiffres du numéro de la carte leur permet, en effet, d'identifier la banque émettrice. Il est même prévu que si la puce se révélait défaillante, les DAB ne puissent pas se contenter des données de la piste magnétique.*

auprès de la banque à chaque opération (du moins, dans les pays disposant d'un réseau de télécommunications fortement développé).

Dès lors, le seul véritable verrou sécuritaire paraît être l'utilisation de la carte à puce.

### 3.- Les données stockées dans la puce

La puce est un circuit électronique miniaturisé, capable de mémoriser des informations et doté de capacités de traitement.

La puce permet de mettre en œuvre trois niveaux d'authentification : celle du porteur, celle de la carte et celle de la transaction.

Il convient de préciser, dès à présent, que les deux premières opérations s'effectuent « hors ligne » (ou « *off line* ») c'est-à-dire sans connexion au réseau interbancaire par une simple communication entre la puce et le terminal (TPE ou DAB). La troisième procédure d'authentification, en revanche, ne peut avoir lieu qu'« en ligne » (ou « *on line* »).

La question qui se pose est donc de savoir si ces trois niveaux ont été détournés par les fraudeurs.

En fait, il apparaît que si l'authentification du porteur et celle de la carte ont déjà pu être cassées, celle de la transaction, en revanche, n'a encore jamais été percée, ce qui autorise le rapport réalisé dans le cadre du Conseil national de la consommation à affirmer que « *les systèmes de carte à puce, tel le système du Groupement des cartes bancaires, paraissent, dans l'état actuel de la technique, être ceux qui garantissent la meilleure protection contre la fraude* ».

- **L'authentification du porteur**

Le code secret à quatre chiffres permet, en principe, d'authentifier auprès de la puce que la personne frappant le code est le possesseur de la carte : la puce vérifie que le code tapé est le même que celui qu'elle stocke.

Cependant, comme cela a déjà été indiqué, ce code peut être assez aisément mis à la disposition de fraudeurs.

- **L'authentification de la carte**

Le deuxième degré sécuritaire de la puce était censé être d'un niveau beaucoup plus élevé que le précédent.

En pratique, la carte s'authentifie comme étant effectivement une carte bancaire auprès du DAB, grâce à un code contenu dans la puce. Cette authentification met en œuvre une cryptographie asymétrique. La carte fournit au terminal son identifiant et une valeur d'authentification (toujours la même pour une carte donnée) qui correspond à cet identifiant chiffré au moment de la création de la carte à l'aide d'un algorithme et d'une clé privée connue du seul GIE cartes bancaires. Le terminal déchiffre alors cette valeur d'authentification à l'aide de la clé publique qu'il contient et vérifie que le résultat obtenu est bien égal à l'identifiant de la carte. La carte n'effectue donc aucun calcul (d'où le terme d'authentification « statique ») : elle ne fait que présenter ces deux données au terminal.

Dans la pratique, cette authentification est la première réalisée. L'authentification du porteur par le code secret n'est demandée qu'à l'issue de l'authentification de la carte.

Ce protocole d'authentification de la carte n'a pas fait l'objet, néanmoins, d'une attention suffisante de la part du GIE cartes bancaires et des banques composant cet organisme et, progressivement, le niveau de protection le concernant a été mis à la portée des « pirates » informatiques. Finalement, en 1999, M. Serge Humpich a réussi à casser cette procédure d'authentification en mettant au point une « *yescard* ». En clair, M. Serge Humpich a trouvé la clé privée mentionnée précédemment et a ainsi pu programmer des cartes à puce vierges, de manière à ce que le terminal accepte l'opération en authentifiant ces cartes pour tout code tapé.

Il convient, néanmoins, de ne pas surévaluer ce « piratage », même si la clé privée a, semble-t-il, été divulguée par la suite sur Internet, car :

– fabriquer une « *yescard* » n'est pas à la portée de tous les fraudeurs. Dans son récent ouvrage [(1)], M. Serge Humpich souligne d'ailleurs, à plusieurs reprises, la difficulté de l'entreprise ;

– cette technique de fraude demeure jusqu'à présent au niveau de la théorie. A l'exception des onze carnets de métro prélevés par M. Humpich pour tester sa découverte, aucun cas de fraude avec cette méthode n'a été recensé par les banques ;

---

*(1) «* Le cerveau bleu *», éditions XO, 2001.*

– un renforcement des mesures cryptographiques assurant la sécurité de l'authentification des cartes bancaires a été mis en œuvre par le GIE cartes bancaires à compter d'octobre 1999.

Les cartes émises depuis cette date sont équipées de clés RSA (Rivest, Shamir, Adleman, du nom des inventeurs de cet algorithme à clé publique) de 768 bits (1) au lieu de 320 bits précédemment.

Selon les éléments recueillis par votre Rapporteur pour avis, des clés de 512 bits ont d'ores et déjà été cassées (2), ce qui implique que la nouvelle norme des cartes bancaires ne devrait résister que quelques années. Toutefois, le passage du standard BO' au standard international EMV (*Europay, MasterCard, Visa*), censé être achevé au 1er mai 2003, devrait éviter ce risque et, comme le nouveau standard sera susceptible d'accepter des clés de l'ordre de 2.000 bits, on peut supposer que les « *hackers* » devront attendre quinze à vingt ans avant d'être en mesure de le casser.

Il n'en demeure pas moins que, tant que les cartes émises avant octobre 1999 seront en circulation (c'est-à-dire compte tenu du renouvellement effectué tous les deux ans, jusqu'en octobre 2001), les terminaux doivent encore accepter les cartes dont la clé utilisée pour leur authentification n'est que de 320 bits ;

– outre que la période d'acceptation des cartes à clé de 320 bits est relativement courte, il importe d'insister sur le fait que les cas où une « *yescard* » peut être utilisée sont, en fin de compte, relativement restreints. Il ne peut s'agir, en effet, que de transactions réalisées « hors ligne », c'est-à-dire sans mise en œuvre du troisième niveau d'authentification, utilisant une clé de chiffrement très différente de celle découverte par M. Serge Humpich.

Une « *yescard* » ne peut donc être acceptée que sur des automates de paiement (distributeurs de billets de métro, de tickets de parking ou péages d'autoroute), des DAB non équipés pour lire la puce (ce qui impliquerait sinon la mise en œuvre des trois types d'authentification) et des TPE travaillant « hors ligne » (généralement pour les opérations inférieures à 600 francs). Dans ce dernier cas, d'ailleurs, une carte vierge ne saurait être acceptée par un commerçant et le fraudeur devrait donc également

---

*(1) Contraction de* Binary Digit *(chiffre binaire), le bit est la plus petite unité d'information manipulable par un ordinateur. Un bit prend la valeur de 0 ou 1.*

*(2) En effet, en août 1999, une équipe de scientifiques de six pays différents, aidés de plusieurs centaines d'ordinateurs, a pu « factoriser » un nombre de 155 chiffres décimaux ! (voir Jacques Stern, « Cryptologie et sécurité informatique : de la guerre des codes au commerce électronique », conférence de l'Université de tous les savoirs publiée dans «* Qu'est-ce que les technologies ? *», éditions Odile Jacob, 2001).*

reproduire le visuel d'une véritable carte. Or, comme le note le rapport du groupe technique restreint : « *une carte plastique est au moins aussi difficile à reproduire qu'un billet de banque* ».

- **L'authentification de la transaction**

Cette procédure réalisée « en ligne » consiste à s'assurer auprès du réseau interbancaire que la carte est rattachée à un compte valide et qu'elle ne figure pas dans la liste des cartes volées ou perdues, liste mise à jour quotidiennement.

La clé mise en œuvre à ce stade n'a jamais été cassée (1). Elle repose sur une cryptologie dite symétrique, utilisant donc, aux deux extrémités de la chaîne, une même clé secrète (et non pas une clé publique et une clé secrète, comme dans la cryptologie asymétrique) cryptée actuellement par un algorithme « DES » (*Data Encryption Standard*) (2) et, lorsque le nouveau réseau d'autorisation sera mis en place, à compter du second trimestre 2002, par un algorithme « triple DES ».

**La carte à puce est donc incontestablement un moyen de paiement très fiable** (3). Encore faut-il que les terminaux soient au même niveau de sécurité.

## 4.- Les terminaux

« *C'est en détaillant l'apparence d'un terminal de paiement que j'ai décidé de faire mes recherches sur la carte bancaire* ». Cette phrase tirée de l'ouvrage de M. Serge Humpich (4) traduit bien l'importance des terminaux dans la sécurité des cartes bancaires.

---

*(1) Dès lors, les propos du général Jean-Louis Desvignes, tenus le 8 mars 2000, alors qu'il était le chef du service central de la sécurité des systèmes d'information, et affirmant que la technologie des cartes à puces devient relativement accessible, apparaissent largement exagérés et imprudents.*

*(2) Pour apprécier les capacités actuelles pour déjouer les protections, on peut signaler que, dès les années quatre-vingt, l'algorithme DES permettant soixante-douze millions de milliards de combinaisons ( ! ! !) était à la portée des ordinateurs de l'Agence de sécurité américaine (NSA). En 1998, une association sans but lucratif, l'*Electronic Frontier Foundation*, a fait construire pour 250.000 dollars une machine capable d'effectuer un décryptement DES en moins d'une semaine (voir le texte de M. Jacques Stern, précité).*

*(3) Outre les trois niveaux d'authentification qu'elle permet de réaliser, il convient d'insister sur le caractère inviolable de la puce en elle-même : nul n'est en mesure aujourd'hui de lire ou d'écrire à l'intérieur d'une puce, comme l'a attesté récemment M. Roland Moreno en offrant, le 13 mars 2000, un million de francs à quiconque réussirait, dans les trois mois, à effectuer l'une de ces opérations. Ce pari n'a pu être relevé.*

*(4) «* Le cerveau bleu *», page 12.*

Cela est pleinement confirmé par le rapport du groupe technique restreint, observant que « *le TPE est (…) un carrefour d'informations, qui est beaucoup plus facile à aborder pour un électronicien qu'une carte à puce. Il est, en outre, programmable. Ces propriétés font qu'un technicien habile peut, à partir d'un TPE modifié, disposer d'informations sur les échanges entre la carte, les modules de vérification du terminal et le réseau, voire recueillir un code en clair au moment où le porteur le frappe sur le clavier* ».

Les TPE ne sont pas seuls concernés. Il a déjà été indiqué que le maintien de DAB non équipés pour lire la puce a pu favoriser certains types de fraude. De même, l'insuffisante réflexion sur la conception de ces appareils rend possible des fraudes mécaniques, du type « collet marseillais ».

Ces problèmes de conception se retrouvent également sur les publiphones. M. Serge Humpich relate ainsi qu'il a pu « *débiter une première carte avec le code d'une deuxième* » en introduisant une languette dans la fente, le temps de procéder à la substitution des cartes.

Il semble effectivement – et cela est profondément regrettable – que la sécurisation des terminaux ait bénéficié de moins d'attention que celle de la carte à puce, comme l'atteste d'ailleurs le nombre de fabricants sur ce marché, largement sous-traité.

Outre, les problèmes de conception « *la question de la mise à niveau des terminaux est un aspect important de toute évolution du système de paiement par cartes* ». Après avoir formulé cette observation, le rapport du groupe technique restreint poursuit : « *les cartes, dont la durée de vie est de deux ans pour les cartes « CB », peuvent évoluer à ce rythme, et sont toujours de version homogène ; par contre, les terminaux, dont la durée de vie est très variable selon les marques, les fonctionnalités et le régime de propriété, forment un parc très hétérogène dont la mise à jour est beaucoup plus lente* ».

Votre Rapporteur pour avis aura l'occasion, dans la suite de ce rapport, de revenir sur la nécessaire mise à niveau des terminaux.

### C.- UNE APPROCHE REPRESSIVE

La fraude à la carte bancaire relève-t-elle de la « délinquance de cour de récréation » ou de la criminalité organisée ?

Incontestablement, certaines techniques de fraude sont relativement simples à mettre en œuvre (en particulier celles liées à la vente à distance et, notamment, à la téléphonie mobile). D'autres techniques, beaucoup plus élaborées telle que le pillage des bases de données, semblent encore être le fait de personnes isolées cherchant un profit immédiat en faisant « chanter » la société volée.

Il serait dangereux néanmoins de n'y voir qu'une délinquance anodine, car, d'une part, cela reviendrait parfois à minorer l'importance de la délinquance chez les jeunes et, d'autre part, cela risquerait de masquer le fait que, de source policière, même si l'on ne dispose pas de statistiques sur ce point, la criminalité organisée est probablement responsable de la majeure partie de la fraude (en montant).

En février 2000, la branche française d'un groupe de fraudeurs de nationalité ivoirienne a été démantelé. Ils utilisaient le réseau Internet de leur cité universitaire pour commander des montres de luxe et surtout des billets d'avion à l'aide de numéros de cartes relevés dans les grands hôtels d'Abidjan [(1)].

Cependant, il semblerait que les principaux groupes organisés dans la fraude à la carte bancaire se situent dans le sud-est asiatique (les triades chinoises) et dans les pays de l'est. Certains groupes terroristes (en particulier, les islamistes basés à Londres) utiliseraient également ces procédés pour assurer leur financement.

Il convient néanmoins de ne pas céder à la tentation du sensationnalisme. La carte à puce possède toutes les conditions pour figurer parmi les instruments de paiement les plus fiables. A cet égard, il est particulièrement significatif qu'American express mène actuellement une campagne de publicité sur la carte à puce « *blue* » alors que pendant très longtemps les Américains se sont contentés de cartes à piste magnétique.

## III.- UNE FRAUDE DONT IL NE FAUT PAS EXAGERER LA PORTEE

La virulence de certaines attaques à l'encontre des cartes bancaires laisse à penser que leurs auteurs perdent de vue que la sécurité absolue en matière de moyens de paiement est illusoire. De plus, les divers intervenants dans le secteur de la carte bancaire ne sont pas dépourvus de moyens pour faire face à la récente recrudescence de la fraude.

---

*(1)* Le Monde *du 27 janvier 2001*

## A.- L'IMPOSSIBLE SECURITE ABSOLUE

Les cartes bancaires ne sont pas le seul instrument de paiement à faire l'objet de fraude et une comparaison avec la situation constatée à l'étranger autorise à nuancer les critiques émises ces deux dernières années.

• **Une fraude concernant l'ensemble des instruments de paiement**

En 1999, on estimait à 250 millions de francs les espèces contrefaites saisies (ne représentant donc qu'une partie de celles en circulation) par l'office central de répression du faux-monnayage.

Pour la même année, le volume d'impayés liés à des paiements par chèque était estimé à 15 milliards de francs, dont une large partie restait définitivement à la charge des commerçants (ce qui est le cas, il convient de le rappeler, dans la majeure partie des fraudes par carte bancaire en situation de paiement à distance).

Les dernières statistiques fournies par le Conseil de sécurité intérieure de janvier 2001 comportent également des données intéressantes sur les infractions relatives au chèque, le mode de paiement préféré des Français.

On y apprend ainsi que les falsifications et usages de chèques volés [(1)] sont également en progression (+5,31% entre 1999 et 2000) et que, même si cette hausse est sensiblement inférieure à celle des falsifications et usages de cartes de crédit (+25,23%), elles sont beaucoup plus nombreuses que ces dernières en valeur absolue : 114.346 falsifications et usages de chèques volés ont été recensés en 2000, contre 48.997 « falsifications et usages de cartes de crédit » [(2)].

Par ailleurs, lors de son audition par votre Rapporteur pour avis, la Fédération des entreprises de vente à distance (FEVAD) a indiqué que les paiements par carte bancaire posent problème pour 0,2% du chiffre d'affaires de ce secteur, tandis que cette proportion s'élève à 1,7% pour les paiements par chèque.

---

*(1) Cette catégorie d'infractions ne recouvre pas les chèques sans provision, dépénalisés depuis la loi n° 91-1382 du 30 décembre 1991 et ne recouvre pas non plus les infractions à la législation sur les chèques (16.619 infractions de ce type ont été recensés en 2000, soit +7,39% par rapport à 1999).*

*(2) Ces termes retenus par le ministère de l'intérieur pour qualifier les infractions qui nous intéressent, sont quelque peu impropres, dans la mesure où la majeure partie des cartes en circulation ne donnent pas à leurs titulaires le bénéfice d'une ouverture de crédit.*

- **Une fraude qui n'est pas spécifique à la France**

La comparaison avec l'étranger est difficile à réaliser, dans la mesure où la France est à peu près le seul pays à pouvoir centraliser ses statistiques de la fraude, du fait de l'existence de la structure interbancaire du GIE.

Lors de son audition par le groupe de travail fonctionnant sous l'égide du Conseil national de la consommation, le GIE a fait valoir que la fraude en Grande-Bretagne était huit fois plus élevée qu'en France en 1999.

Le groupe allemand Euro Kartensysteme, rattaché au réseau Eurocard, estimait récemment que l'Allemagne avait connu en 2000 une augmentation de 32% des cas de fraude lors du paiement par carte bancaire sur Internet.

Pour les Etats-Unis, selon une note de l'ambassade de France, les estimations citées en matière de fraude sont variables : « *Une société d'étude spécialisée dans le domaine du commerce électronique,* Celent Communications*, évaluait fin décembre 2000, que la fraude aura coûté aux détaillants en ligne 1 milliard de dollars en 2000, dont 300 millions au seul titre des achats effectués au cours des fêtes de fin d'année. Cette société estimait par ailleurs que le taux de fraude est 30 fois supérieur sur Internet à celui observé chez les détaillants traditionnels : il représente 3% des ventes dans le premier cas et 0,1% dans le second. Pour d'autre sources, les détaillants sur Internet perdent entre 1 et 6% de leur volume de transactions. Selon le cabinet d'études* GartnerGroup*, la fraude par carte de crédit porte sur plus d'1% des transactions sur Internet, elle est 12 fois supérieure à celle des transactions effectuées en personne.* BAI Global Inc*, société d'études de marché, estime que 10% des Américains ont été victimes de fraude par carte de crédit, que la fraude sur des cartes de débit ou de distributeurs automatiques de billets affecte 7% des Américains et enfin, que sans avoir jamais perdu de carte, 5% des Américains ont été victimes de fraudes.* »

Ces chiffres, beaucoup plus élevés que ceux annoncés par Visa, peuvent expliquer que les cartes à puce sont apparues de façon significative courant 1999 au Etats-Unis. American express y a introduit sa carte « *blue* » en septembre 1999 (elle était distribuée en Grande-Bretagne depuis 1998). Trois émetteurs d'importance (*Providian Financial Corp*., *Fleet Boston Financial Corp.* et *First USA*) ont émis des cartes à puce sous le logo Visa. Enfin, des cartes à puce MasterCard doivent être diffusées en 2001. Cependant, l'infrastructure américaine doit également être adaptée, les

détaillants n'étant pas encore équipés de terminaux de paiement acceptant les puces électroniques.

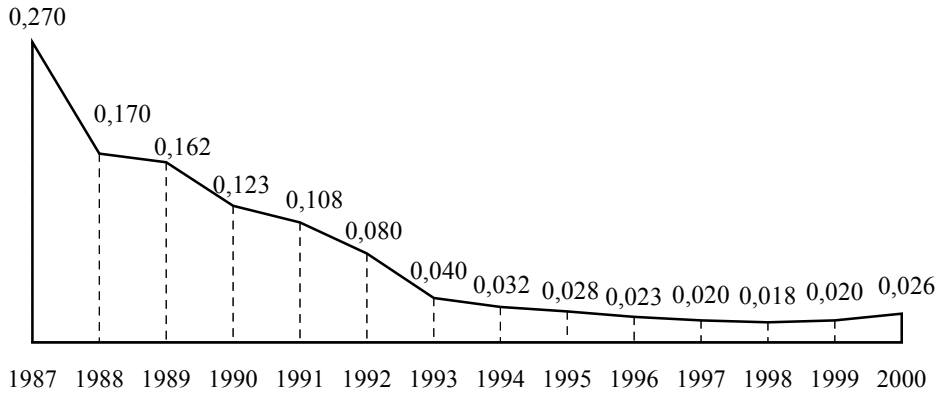
- **Une fraude sensiblement moins forte que par le passé**

Malgré les réserves qui ont pu être formulées à l'encontre des statistiques fournies par le GIE cartes bancaires, il s'agit d'une série continue, établie selon des critères identiques d'une année sur l'autre, dont l'évolution n'est donc pas dénuée de signification.

Or, cette évolution traduit une réduction très importante du taux de fraude sur les paiements réalisés en France de 1987 à 1998 (de 0,27% en 1987 à 0,018%), avant une faible remontée en 1999 et 2000.

**TAUX DE FRAUDE SUR LES PAIEMENTS** (a)

*(en %)*




(a) Taux de fraude = montant des transactions frauduleuses, rapporté au montant total des paiements par cartes « CB » en France.

*Source : GIE cartes bancaires.*

Encore une fois, ces données ne concernent que la fraude sur les paiements (ce qui exclut les fraudes sur les DAB et notamment les problèmes de « *white plastic* ») réalisés en France (on ne tient donc pas compte de la forte hausse de la fraude sur les cartes « CB » à l'étranger) et supportée par les banques (à l'exclusion, en conséquence, de la fraude sur les ventes à distance, à la charge des commerçants, et d'une partie de la fraude effectuée avant la mise en opposition de la carte perdue ou volée).

Il n'en demeure pas moins que la baisse du taux de fraude enregistrée au début des années quatre-vingt-dix – grâce essentiellement à la diffusion de la carte à puce – est loin d'être négligeable.

Cette baisse est également perceptible si l'on compare le nombre des infractions relatives aux falsifications et usages de cartes, recensées par les services de police et de gendarmerie, d'une part, avec le nombre total des paiements et des retraits réalisés avec des cartes bancaires « CB ». Cette comparaison, qui ne saurait permettre d'établir un véritable taux de fraude, dans la mesure notamment où toutes les victimes ne déposent pas une plainte et où les paiements et retraits effectués avec des cartes d'autres émetteurs ne sont pas pris en compte, illustre bien, néanmoins, la diminution du risque de fraude au cours des années quatre-vingt-dix.

**NOMBRE DE FALSIFICATIONS ET USAGES DE CARTES DE CREDIT**

| | **1990** | **1991** | **1992** | **1993** | **1994** | **1995** | **1996** | **1997** | **1998** | **1999** | **2000** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| I.- Nombre d'infractions | 46.981 | 43.947 | 40.466 | 32.568 | 34.886 | 28.295 | 27.477 | 27.860 | 30.459 | 39.126 | 48.997 |
| II.- Nombre de retraits et de paiements par cartes bancaires « CB » *(en millions)* | 1.264 | 1.846 | 2.008 | 2.188 | 2.337 | 2.585 | 2.850 | 3.137 | 3.486 | 3.930 | 4.363 |
| I/II *(en %)* | 0,0029 | 0,0027 | 0,0022 | 0,0016 | 0,0016 | 0,0012 | 0,0010 | 0,0009 | 0,0009 | 0,0011 | 0,0012 |

En outre, dans certains domaines exclus des statistiques du GIE, les opérateurs ont déjà su prendre des mesures de bon sens qui ont permis un recul conséquent du taux de fraude qu'ils avaient enregistré précédemment.

## B.- DES SUCCES DEJA ENREGISTRES DANS LA LUTTE CONTRE LA FRAUDE

Les opérateurs de téléphonie mobile ont subi, à compter de fin 1998, une importante fraude sur les cartes prépayées à rechargement à distance (à l'exception d'Itinéris, qui ne s'était pas engagé sur ce marché). Leur taux d'impayés (en valeur) sur les rechargements effectués par carte bancaire a ainsi atteint plus de 11% et il importe de rappeler que le taux de fraude donné par le GIE cartes bancaires pour l'ensemble des opérations à distance et pour le premier semestre 2000 (un taux de 0,11%) était imputable pour moitié à ces opérations de rechargement de téléphonie mobile.

Pourtant, fin 2000, le taux d'impayés n'est plus que de l'ordre de 1,5%. Les opérateurs qui supportaient la charge de la fraude ont, en effet, su réagir en quelques mois grâce à de simples mesures d'ordre organisationnel.

A titre d'exemple, le tableau suivant retrace les mesures mises en place par Cegetel pour lutter contre la fraude sur les cartes prépayées SFR.

**MESURES ANTI-FRAUDE ADOPTEES PAR SFR**

| | |
|---|---|
| Depuis 1998 | Mise en place d'une liste noire des numéros de carte bancaire utilisés frauduleusement : inscription dès la première répudiation |
| 5 mai 2000 | Réduction du seuil mensuel maximum de rechargement par carte bancaire pour chaque ligne (de 575 F à 289 F) |
| 25 mai 2000 | Réduction de 3 à 1 du nombre maximum de cartes bancaires utilisable sur une ligne sur 3 mois<br>Réduction de 3 à 2 du nombre maximum de lignes pouvant être rechargées par une carte bancaire sur 3 mois |
| Mai 2000 | Décision de ne pas proposer la maxi-recharge (2h+2h) en vente à distance |
| 3 juillet 2000 | Refus d'identification en ligne d'un nouveau client au service clients : les identifications ne sont faites que sur papier |
| 11 juillet 2000 | Blocage du rechargement par carte bancaire aux clients non identifiés |
| 1er septembre 2000 | Blocage du rechargement par carte American express (plus de 20% d'impayés sur cette carte)<br>Blocage du rechargement par carte étrangère (95% d'impayés) |

*Source : Cegetel.*

Il s'agit, comme on le constate, de mesures de simple bon sens, évitant de faciliter la tâche des fraudeurs ou de rendre la fraude trop tentante. Les résultats sont probants mais l'effort doit être poursuivi avec l'appui des banques et du GIE.

Ces derniers ont d'ailleurs, d'une façon générale, trop tardé à adopter des mesures simples qui auraient pu éviter, ou tout au moins atténuer, la recrudescence de la fraude à la carte bancaire et le préjudice que sa médiatisation a pu causer à cet instrument de paiement. Il a fallu que le Gouvernement se saisisse du dossier au printemps dernier pour que, enfin, des mesures pertinentes soient annoncées et mises en œuvre.

## CHAPITRE III

## DES MESURES DE SECURISATION PERTINENTES

Les possibles implications monétaires et économiques de la mise en cause, auprès du grand public, de la sécurité de la carte bancaire, ainsi que les conséquences de la hausse de ce type de fraude sur les statistiques de la criminalité en 2000, ont conduit le Gouvernement à s'impliquer directement dans ce dossier.

Cette implication a, tout d'abord, revêtu la forme d'une table ronde, réunie, le 4 avril 2000, par Mme Marylise Lebranchu, alors secrétaire d'Etat aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation, et rassemblant tous les acteurs concernés par les cartes de paiement. A l'issue de cette réunion, un mandat a été confié à un groupe de travail, dans le cadre du Conseil national de la consommation, pour établir un état des lieux des difficultés rencontrées sur les paiements par carte et formuler des recommandations simples et opérationnelles visant à limiter le risque de fraude.

Compte tenu de la technicité de la matière, un autre groupe de travail, dit « groupe technique », animé par la mission « commerce électronique » du ministère de l'économie, des finances et de l'industrie, avec la participation des services du Premier ministre (Secrétariat général de la défense nationale et Direction centrale de la sécurité des systèmes d'information), a été constitué pour assister le groupe de travail fonctionnant sous l'égide du Conseil national de la consommation.

Par ailleurs, un groupe de travail interministériel, animé par la Direction du trésor, a été constitué à l'été 2000 pour examiner les aspects juridiques, notamment pénaux, de la lutte contre la fraude aux cartes bancaires.

S'appuyant sur les travaux de ces trois groupes de travail, M. Laurent Fabius, ministre de l'économie, des finances et de l'industrie, a annoncé, le 22 février 2001, anticipant la remise officielle du rapport rédigé dans le cadre du Conseil national de la consommation, un « *premier train de mesures* », comprenant des dispositions de nature législative, d'une part, et deux « chartes » par lesquelles les professions concernées prennent de nombreux engagements, d'autre part.

L'étude de ce dispositif doit être complétée par un rappel des diverses initiatives internationales concernant ce problème, puisque la sécurité des cartes de paiement ne saurait être traitée au seul plan national.

## I.- DES MESURES LEGISLATIVES, DONT LA NECESSITE S'IMPOSE

Le présent projet de loi relatif à la sécurité quotidienne comporte un chapitre III regroupant six articles modifiant le code monétaire et financier, visant à améliorer la sécurité des cartes de paiement. Ces dispositions sont complétées par l'article 16, adaptant les dispositions prévues par l'article 8 à la situation spécifique des départements d'outre-mer.

Il convient, tout d'abord, de souligner qu'une intervention législative dans ce domaine n'est pas fréquente. En fait, jusqu'à la loi n° 91-1382 du 30 décembre 1991 précitée, qui a défini les cartes de paiement et de retrait, affirmé l'irrévocabilité de l'ordre de paiement par carte et prévu des sanctions en cas de contrefaçon et de falsification, il n'existait pas de législation spécifique à cette matière essentiellement régie par le droit contractuel.

Le dispositif proposé par le chapitre III et l'article 16 précités constitue donc la seconde intervention d'importance du législateur. Celle-ci se situe à trois niveaux, puisqu'elle vise à renforcer la prévention de la fraude, sa répression et la protection des consommateurs.

### A.- PREVENIR : L'ACCROISSEMENT DU ROLE DE LA BANQUE DE FRANCE

Les mises en cause, ces deux dernières années, de la sécurité des cartes bancaires ont permis de mettre en évidence les défaillances du Groupement des cartes bancaires. En prévoyant un renforcement du rôle de la Banque de France et de l'Institut d'émission d'outre-mer, **les articles 8 et 16 du présent projet de loi** tirent logiquement les conséquences de cette constatation.

## 1.- Le Groupement des cartes bancaires : une structure nécessaire mais défaillante

### *a) Une structure nécessaire*

Les principes qui régissent l'organisation et le fonctionnement du Groupement des cartes bancaires et le système de paiement par carte mis en place dans le cadre de ce groupement, sont définis dans trois textes de base : le protocole d'accord de 31 juillet 1984 entre les banques « carte bleue », le Crédit agricole et le Crédit mutuel ; le contrat constitutif du Groupement signé le 30 novembre 1984 et le règlement intérieur du Groupement.

Le Groupement est un groupement d'intérêt économique, régi par l'ordonnance du 23 septembre 1967. Il s'agit d'une personne morale de droit privé, qui n'est dotée d'aucune prérogative de droit public, ni de pouvoir réglementaire propre. Il emploie environ 220 personnes, pour un budget annuel de l'ordre de 300 millions de francs.

L'article 3 du contrat constitutif précité prévoit que le Groupement a pour objet :

– d'assurer l'étude, la normalisation, la promotion, la représentation, la sécurité et la prévention des fraudes, du système interbancaire des cartes « CB » ;

– d'organiser l'acceptation des cartes agréées « CB » dans le système « CB » ;

– de mettre en œuvre et d'assurer la gestion de tous les services communs nécessaires à l'interbancarité et à l'interopérabilité du système « CB » avec les systèmes de cartes agréées « CB » et/ou avec ceux avec lesquels le Groupement a passé un accord ;

– d'exercer toute activité de prestations de services ou d'agrément et de qualification liée à l'activité monétique « CB » ;

– d'assurer en justice la représentation collective ou individuelle de ses membres, notamment aux fins d'obtenir réparation du préjudice subi par eux individuellement ou collectivement à l'occasion de fraudes et/ou de tout autre dommage de quelque nature qu'il soit, au titre des activités « CB » ; le Groupement a également le pouvoir de transiger et de compromettre ;

– d'assurer, à la demande de certains de ses membres et à titre accessoire, la gestion de services supplémentaires liés à l'activité monétique du Groupement ;

– de veiller à l'intégrité et à la sécurité des applications « CB » sur les cartes multi-applicatives ;

– et plus généralement, de faire toute opération de quelque nature que ce soit, nécessitée par l'activité monétique du Groupement qu'elle soit notamment économique, juridique ou financière, y compris des prises de participation directe ou indirecte.

Pour mettre en œuvre ses missions, le Groupement est organisé autour de onze « chefs ce file » [(1)], en fait les principales banques ou établissements de crédit parmi les 175 qui le composent. Ces onze établissements constituent le conseil de direction du Groupement. La Banque de France participe à ce conseil de direction en tant qu'observateur. L'application des directives de ce conseil est mise en œuvre par un administrateur.

Le GIE fait l'objet de nombreuses critiques, mais son utilité n'est jamais véritablement contestée, car :

– d'une part, il rend possible l'interbancarité en assurant la gestion du réseau téléinformatique d'autorisation ;

– d'autre part, il constitue un interlocuteur unique (du moins, réunissant un grand nombre d'émetteurs de cartes de paiement), ce qui lui permet de centraliser de multiples informations et en fait un collaborateur apprécié des services policiers chargés de la lutte contre la fraude.

*b) Une structure défaillante*

La composition du conseil de direction du GIE, traduit assez fidèlement sa vocation. Il s'agit d'un instrument faisant prévaloir les intérêts des grands groupes bancaires. Ces intérêts particuliers vont parfois à l'encontre de l'intérêt général, comme l'attestent deux décisions du Conseil de la concurrence et – surtout – l'approche strictement financière adoptée par le GIE en matière de fraude.

Ainsi, par une décision n° 88-D-37 du 11 octobre 1988, le Conseil de la concurrence a notamment enjoint au GIE de cesser de fixer une

---

*1) BNP Paribas, Caisses d'épargne, CCF, CIC, Crédit agricole, Crédit du Nord, Crédit lyonnais, Crédit mutuel, La Poste, Natexis Banques populaires, Société générale.*

tarification minimum des cotisations mises à la charge des porteurs. Il lui a également imposé d'accorder un délai raisonnable aux commerçants adhérant au système national de paiement par carte pour accepter toute modification des conditions particulières de leur contrat. Pour l'essentiel, le Conseil de la concurrence a exigé que le Groupement modifie les modalités de calcul du prélèvement effectué par les banques sur les commerçants affiliés (la commission interbancaire de paiement). Or le Groupement s'est plié de mauvaise grâce à cette dernière injonction et, par sa décision n° 90-41 du 30 octobre 1990, le Conseil de la concurrence lui a infligé une sanction pécuniaire de six millions de francs. Il convient, néanmoins, d'observer que, par une lettre du 30 octobre 2000, la direction générale de la concurrence de la Commission européenne a considéré, au terme d'une procédure ayant duré douze ans, que les règles de coopération interbancaires « CB » n'ont pas d'effet sur le commerce entre les Etats membres et ne restreignent pas sensiblement la concurrence.

En matière de lutte contre la fraude, la position du Groupement est parfaitement exprimée par la phrase suivante, tirée d'un document de présentation du système cartes bancaires « CB » remis à votre Rapporteur pour avis lors d'une audition du GIE : « *La fraude est considérée comme insupportable au-delà de 0,03%-0,04% du montant des paiements* ».

*A contrario*, un taux de fraude inférieur (le taux actuel, rappelons-le, est de 0,026% pour les paiements en France par cartes « CB ») serait donc supportable et n'inciterait pas le Groupement et ses membres à prendre toutes les précautions nécessaires.

Il serait cependant injuste d'affirmer que le Groupement ne lutte pas contre la fraude. Il dispose même, depuis 1999, d'une cellule de gestion des risques. Mais, il a fait preuve, selon sa propre expression, d'« *une forte inertie intrinsèque* » [(1)], qui a été particulièrement flagrante en ce qui concerne le rallongement de la clé utilisée lors de l'authentification de la carte et la modernisation des DAB.

Dès 1988, c'est-à-dire avant même que le Groupement ne prenne la décision d'équiper toutes les cartes de paiement d'une puce, MM. Louis Claude Guillou (l'un des concepteurs de la carte bancaire à puce), Marc Davio et Jean-Jacques Quisquater indiquent que « *des fraudeurs pourront bientôt produire des valeurs d'authentification, conformes à celles issues*

---

*(1) Courrier de M. Yves Randoux, Administrateur du GIE, adressé à votre Rapporteur pour avis le 29 mars 2001.*
*On peut ajouter que le GIE n'est pas le seul émetteur de cartes à adopter une approche financière de la sécurité. Ainsi, Cofinoga ne souhaite pas équiper ses cartes d'une puce car cela coûte cinq francs par carte («* Le courrier de la monétique et de la carte à mémoire *», juin 2000, p. 29).*

*aujourd'hui par* (sic) *l'autorité bancaire* » [1]. Pourtant, le GIE ne procéda pas à l'allongement des clés de 320 bits. Selon les informations transmises par le Groupement à votre Rapporteur pour avis, « *en 1998, bien avant que n'éclate l'affaire Humpich, un plan sécuritaire avait été arrêté par les banques, mais en raison de l'arrivée proche de l'euro ce plan avait été décalé, car aucune menace sérieuse ne pesait sur le système* ».

Grave erreur d'appréciation puisqu'en 1999, l'affaire Humpich faisait la « une » des journaux – en partie, d'ailleurs, à cause de la mauvaise gestion de ce dossier par le GIE – et contribuait à développer le doute sur la sécurité de la carte bancaire. Des économies de bouts de chandelle ont ainsi fragilisé cet instrument de paiement.

De la même façon, le GIE disposait, depuis des années, d'un moyen efficace de lutte contre la fraude à la « *white plastic* ». Cette dernière est surtout « facile » à mettre en œuvre sur les DAB, car il n'est pas nécessaire que la carte utilisée possède le visuel d'une véritable carte. Néanmoins, elle n'est possible que sur les DAB se contentant de lire la piste magnétique et qui ne sont donc pas équipés pour lire la puce. Une généralisation des DAB traitant la puce aurait donc permis de réduire singulièrement le champ d'application de la « *white plastic* ». Pourtant, selon le rapport réalisé dans le cadre du Conseil national de la consommation, 25% des DAB seulement lisaient la puce des cartes au début 2000. Là encore, ce n'est qu'après la diffusion d'informations alarmantes sur les cartes bancaires et la hausse sensible des retraits frauduleux, que le Groupement s'est décidé à réagir : au 1er janvier 2001, 67% des DAB traitaient la puce et ce pourcentage atteignait 84% fin mars 2001 (en juin, la totalité des DAB seront équipés).

Il n'est pas contestable que ces travaux d'équipement ont un coût : le Groupement l'estime à environ 10.000 francs pour chacun des DAB, ce qui globalement, représente un investissement de l'ordre de 300 millions de francs. Le Groupement, lors de son audition par le groupe de travail œuvrant sous l'égide du Conseil national de la consommation, a mis ce dernier chiffre en relation avec les 61 millions de francs qu'ont représenté, en 1999, les fraudes sur les retraits. Cette comparaison est hautement contestable car, d'une part, elle devrait plutôt prendre en compte le montant de la fraude sur l'ensemble des années où les DAB nouvellement équipés seront en service (il convient de rappeler qu'en 2000, cette fraude a atteint 70 millions de francs) et, d'autre part, elle participe – encore une fois – d'une vision strictement financière de la gestion d'un instrument de paiement qui, par nature, ne saurait être considéré comme un produit bancaire banal. Il y a d'ailleurs fort à parier que, sans la médiatisation de ce dossier, le GIE se

---

*(1)* Annales des télécommunications*, n°9-10, 1988.*

serait abrité derrière la nécessité d'adapter les DAB à l'euro et même derrière les obligations d'aménagement liées à la sécurisation des transports de fonds, pour différer la généralisation des DAB lisant la puce.

C'est donc à juste raison que le Gouvernement a décidé de consolider le rôle de la Banque de France, pour que la puissance publique puisse exercer pleinement son rôle de sécurité.

## 2.- Le rôle consolidé de la Banque de France

Le rapport réalisé dans le cadre du Conseil national de la consommation a préconisé aux pouvoirs publics d'« *examiner les conditions d'implication de la Banque de France dans la sécurité des moyens de paiement* ». Les articles 8 et 16 du présent projet de loi mettent en œuvre cette recommandation et visent à donner une assise juridique explicite aux interventions de la Banque de France (ainsi que de l'Institut d'émission d'outre-mer, en ce qui concerne les départements d'outre-mer).

### *a) L'implication actuelle de la Banque de France*

Aux termes de l'article 105, paragraphe 2, du Traité instituant la Communauté européenne, « *les missions fondamentales relevant du Système européen de banques centrales* (SEBC) *consistent à* […] *promouvoir le bon fonctionnement des systèmes de paiement* ».

A l'occasion de l'adaptation du statut de la Banque de France aux dispositions du Traité, le législateur a précisé que « *la Banque de France veille au bon fonctionnement et à la sécurité des systèmes de paiement, dans le cadre de la mission du Système européen de banques centrales relative à la promotion du bon fonctionnement des systèmes de paiement* » (article 4 de la loi n° 93-980 du 4 août 1993, codifié à l'article L. 141-4 du code monétaire et financier).

Ainsi que l'indique la Déclaration de la Banque centrale européenne sur le rôle de l'Eurosystème en matière de surveillance des systèmes de paiement [(1)], les compétences dans ce domaine sont donc exercées conjointement par la Banque centrale européenne (BCE) et les banques centrales nationales (BCN). Le cadre général de la surveillance est défini par le Conseil des gouverneurs de la BCE. Les BCN sont chargées de la mise en œuvre de la surveillance des systèmes domestiques et il revient au Conseil de statuer sur la surveillance des systèmes internationaux.

---

*(1) Déclaration publiée le 21 juin 2000.*

La surveillance menée par la Banque de France s'exerce, notamment, par sa participation aux travaux du Comité français d'organisation et de normalisation bancaires (CFONB), qui est non seulement en charge de la normalisation mais aussi de nombreuses réflexions sur l'organisation du système de paiement, et à toutes les instances dirigeantes des organismes responsables de la gestion de systèmes de paiement ou d'instruments de paiement (notamment le bureau et le conseil de direction du GIE en charge du Système interbancaire de télécompensation, l'assemblée générale ordinaire de la Centrale des règlements interbancaires et, comme cela a déjà été signalé, le conseil de direction du Groupement des cartes bancaires).

L'activité de surveillance s'est également étendue au cours des dernières années à la monnaie électronique. En 1998, l'Eurosystème a publié un rapport sur la monnaie électronique qui a fixé un certain nombre d'exigences minimales concernant ces instruments de paiement. La Banque de France a, par ailleurs, contribué, en coopération avec la Direction centrale de la sécurité des systèmes d'information (DCSSI), les professionnels du domaine et les établissements de crédit, à la réalisation d'un cahier des charges permettant une évaluation formelle des porte-monnaie électroniques dans le cadre d'un schéma national d'évaluation et de certification de la sécurité des systèmes d'information.

S'agissant plus spécifiquement des cartes bancaires, il a déjà été indiqué que la Banque de France bénéficie d'un poste d'observateur au sein de l'instance de décision du Groupement des cartes bancaires, le conseil de direction [(1)]. Elle participe également au comité « gestion des risques » chargé de l'analyse des risques sur le système « CB » et de la lutte contre la fraude.

Lorsque des décisions lui paraissent de nature à compromettre la sécurité du système et la confiance des utilisateurs, la Banque de France manifeste son opposition au sein du conseil de direction, où son autorité morale est censée lui permettre de peser sur les prises de position des participants. La Banque de France peut également, si elle l'estime nécessaire, intervenir directement auprès des responsables du Groupement ainsi que des directions générales des banques « chefs de file » du Groupement.

Il importe de signaler que ce rôle, qui peut apparaître relativement limité, est pourtant plus important que celui dévolu aux autres banques

---

*(1) Il convient de souligner que la présence de la Banque de France en tant qu'observateur au sein du conseil de direction n'est pas mentionnée dans le contrat constitutif du GIE. Elle présente donc un caractère très informel.*

centrales de l'Union européenne en matière de cartes bancaires. Il existe, en effet, une incertitude sur la portée de la notion de « systèmes de paiement », mentionnée par l'article L.141-4 du code monétaire et financier. Il n'est pas certain qu'elle englobe les « moyens de paiement ». Pour écarter ce doute, l'article 8 du présent projet de loi complète l'article L. 1414 précité, afin de prévoir explicitement que « *la Banque de France s'assure de la sécurité des moyens de paiement* ».

*b) Un pouvoir de recommandation à l'égard de l'ensemble des émetteurs*

Le dispositif proposé par le Gouvernement peut faire l'objet de plusieurs observations.

• **La consolidation du rôle de la Banque de France porte sur l'ensemble des moyens de paiement scripturaux**

La Banque de France a déjà pour mission d'assurer l'entretien de la monnaie fiduciaire et de gérer la bonne qualité de sa circulation (article L. 141-5 du code monétaire et financier). Elle est désormais explicitement compétente pour s'assurer de la sécurité non seulement des cartes bancaires mais aussi des chèques, virements, effets de commerce, avis de prélèvement, titres interbancaires de paiement, porte-monnaie électroniques, porte-monnaie virtuels…

• **Le GIE cartes bancaires n'est pas placé sous la tutelle de la Banque de France**

Compte tenu des défaillances précédemment mentionnées du GIE, plusieurs voix avaient demandé que la Banque de France ne se cantonne plus à son rôle d'observateur au sein du GIE et assure une véritable tutelle sur cet organisme.

Cette voie n'a pas été retenue par le Gouvernement, puisque globalement le GIE conserve son rôle d'édiction des normes de sécurité dans le cadre des objectifs définis par la Banque de France.

La mise sous tutelle n'était effectivement pas souhaitable car :

– le Groupement cartes bancaires ne gère qu'une partie des cartes de paiement ; le dispositif proposé permet également de conforter le rôle de la Banque de France auprès des émetteurs de cartes privatives ;

– le GIE doit être considéré comme un interlocuteur crédible lors des négociations internationales qu'il mène avec d'autres émetteurs pour

arrêter les futures normes de sécurité. En ce sens, l'article 8 du présent projet de loi établit un équilibre entre la réaffirmation du rôle de la puissance publique et la préservation des compétences du Groupement.

• **Pour s'assurer de la sécurité des moyens de paiement et de la pertinence des normes applicables en la matière, la Banque de France se voit reconnaître deux attributions nouvelles**

Le texte précise, en effet, que la Banque de France doit, d'une part, procéder aux expertises utiles et, d'autre part, se faire communiquer les informations nécessaires.

Dès lors, il importe :

– de confier à la Banque de France les moyens en hommes et en matériels suffisants pour réaliser ces expertises et de s'assurer de l'indépendance des experts à qui il sera fait appel ;

– de se demander si la Banque de France aura la faculté de se faire communiquer l'ensemble des informations utiles. Néanmoins, en cas de refus, l'émetteur récalcitrant serait exposé aux mesures contraignantes prévues par le présent article.

• **La Banque de France ne peut pas s'opposer, en l'état actuel du texte, à la mise à disposition du public de tout instrument de paiement dont la sécurité serait déficiente**

Contrairement à ce que le ministre de l'économie, des finances et de l'industrie a indiqué lors de son intervention du 22 février 2001 sur l'amélioration de la sécurité des cartes bancaires, le dispositif proposé ne donne pas formellement à la Banque de France un tel pouvoir.

Ses capacités contraignantes vont au-delà de sa seule capacité actuelle de conviction, mais elles se limitent à un pouvoir de simples recommandations et, si ces dernières s'avèrent insuffisantes, à une capacité de formuler un avis négatif, éventuellement rendu public.

Là aussi, le texte peut laisser penser que la Banque de France peut choisir de ne pas rendre public cet avis. Pourtant, seule la possibilité de rendre public son avis apparaît comme une véritable novation. En tant qu'observateur au sein du conseil de direction du GIE cartes bancaires, la Banque de France a déjà la faculté de faire part de ses réserves à l'encontre des décisions adoptées, mais sans qu'aucune publicité soit donnée à ces interventions. Ainsi, dès 1999, la Banque de France a demandé au GIE de ne plus différer l'allongement des clés cryptographiques RSA.

• **Le Gouvernement a également annoncé la mise en place d'un Observatoire de la sécurité des cartes bancaires, dont le secrétariat général sera assuré par la Banque de France**

Cet observatoire qui, en l'état actuel du texte proposé, ne serait pas créé par la loi, devrait regrouper les différents acteurs concernés par ce moyen de paiement (outre les émetteurs, il devrait réunir notamment des représentants des porteurs et des commerçants). Il est conçu comme une instance de dialogue, permettant à chaque partie de mieux intégrer les contraintes de ses interlocuteurs. Il doit assurer, en particulier, le suivi des engagements pris par les banques et le Conseil du commerce de France dans les deux chartes signées le 22 février dernier.

### B.- REPRIMER : UNE NOUVELLE INFRACTION PENALE

Le groupe de travail interministériel, précédemment évoqué, chargé d'étudier les aspects juridiques, notamment pénaux, de la lutte contre la fraude, a constaté que, sur le plan répressif, deux types de textes régissent actuellement les fraudes aux cartes de paiement ou de retrait :

– le code pénal, qui permet de sanctionner des infractions de droit commun, telles que l'escroquerie et les atteintes a des systèmes de traitement automatisés de données ;

– le code monétaire et financier, qui vise spécifiquement les actes de contrefaçon et de falsification. Les articles 10 et 11 de la loi n° 91-1382 du 30 décembre 1991 ont, en effet, introduit des dispositions – désormais codifiées aux articles L. 163-3 à L. 163-5 du code monétaire et financier – prévoyant qu'est puni d'un emprisonnement de sept ans et d'une amende de cinq millions de francs le fait pour toute personne de contrefaire ou de falsifier une carte ; de faire ou de tenter de faire usage, en connaissance de cause, d'une carte contrefaite ou falsifiée ; d'accepter, en connaissance de cause, de recevoir un paiement au moyen d'une carte contrefaite ou falsifiée. En outre, la confiscation, aux fins de destruction, des cartes contrefaites ou falsifiées est obligatoire. De même, est obligatoire la confiscation des matières, machines, appareils ou instruments qui ont servi ou étaient destinés à servir à la fabrication de ces cartes, sauf lorsqu'ils ont été utilisés à l'insu du propriétaire.

Néanmoins, le groupe de travail a surtout observé que ces textes ne permettent pas de réprimer certaines nouvelles formes de la fraude, comme l'illustre le tableau suivant.

**TYPOLOGIE DES FRAUDES ET INCRIMINATIONS**

| Type de fraude | Actes nécessaires à la commission de la fraude | Incriminations |
|---|---|---|
| **I.- FRAUDES SIMPLES** | | |
| **1. Vol de carte et usage** | – Vol simple (pickpocket, courrier…) ou vol avec violences de la carte et parfois du code ou vol par ruse de la carte et parfois du code. | art. 311-1 CP [(a)] |
| | – Utilisation du support, soit dans un DAB, soit auprès d'un commerçant. | art. 313-1 et ss CP |
| **2. Fraude « à la thaïlandaise »** | – Détenir à titre de commerçant un appareil manuel de facturation (dit « fer à repasser ») | |
| | – Constater un encaissement réel au moyen d'une carte bancaire ; prendre l'empreinte de la carte (numéro de carte, nom du porteur, date de validité) et changer de facturette pour procéder à la transaction réelle. | art. L. 163-4 CMF [(b)] |
| | – Conserver la trace de la signature du porteur. | |
| | – Utiliser la première facturette chez un autre commerçant complice et encaissement. | art. L. 163-4 CMF et art. 313-1 CP |
| **3. Recharge de cartes téléphoniques à distance** | – Récupération d'une facturette sur laquelle figurent les 16 chiffres nécessaires.<br>– Utilisation de ce numéro auprès d'un service de téléphonie mobile pour la recharge de cartes sans abonnement. | art. 313-1 et ss CP |
| **4. Achat par correspondance** | – Récupération d'un numéro de porteur de carte de paiement, soit sur une facturette, soit par utilisation d'un logiciel de « moulinage » (déclinaison de numéro).<br>– Utilisation de ce numéro en V.P.C. (minitel, téléphone, fax), ou par Internet.<br>– Usage d'une fausse adresse et d'un faux nom pour les livraisons des marchandises. | art. 313-1 et ss CP |
| **II.-FRAUDE « ASTUCIEUSE »** | | |
| **1. Fausses façades de paiement** | – Fabrication de fausses façades de paiement pour guichet automatique ou automate. | Néant |
| | – Fabrication de logiciels ou supports électroniques de captation et d'enregistrement des données cartes bancaires. | Néant |
| | – Installation de fausses façades et de systèmes de captation des pistes et codes secrets. | art. 313-1 et ss CP |
| | – Captation des données et enregistrements. | |
| | – Détention des supports portant enregistrement des données captées. | |
| | – Détention des matériels ayant servi à la captation. | |
| | – Encodage des numéros sur des supports vierges. | |
| | – Achat et détention de supports vierges nécessaires aux réencodages. | Néant |
| | – Détention des supports encodés. | |
| | – Détention de logiciel d'encodage. | Néant |
| | – Usage des supports encodés dans des guichets automatiques en France. | art. L. 163-4 et ss CMF |
| **2. Piratage de terminaux de paiement** | – Conception et fabrication de logiciels de dérivation de données magnétiques et du code confidentiel. | Néant |
| | – Installation de microprocesseurs et de mémoire dans des TPE. | Néant |
| | – Dédoublement du lecteur-piste du TPE et du PIN-PAD (clavier) | Néant |
| | – Installation des TPE chez des commerçants (complices ou non) | art 313-1 et ss CP |
| | – Captation des données au fur et à mesure des transactions et enregistrement et transmission. | art 313-1 et ss CP |
| | – Détention des données piratées, soit sur listing papier, soit sur mémoire informatique. | Néant |
| | – Encodage de supports vierges | art. L. 163-4 et ss CMF |
| | – Utilisation des supports dans les DAB. | art. L. 163-4 et ss CMF |

| Type de fraude | Actes nécessaires à la commission de la fraude | Incriminations |
|---|---|---|
| **3. Falsification de cartes volées** | – Détention de matériels spécifiques destinés à l'aplatissage, l'embossage et l'encodage. | Néant |
| | – Détention de cartes volées. | art. 321-1 et ss CP |
| | – Falsification, utilisation et acceptation de cartes falsifiées (l'acceptation doit être intentionnelle pour être incriminée). | art. L. 163-4 et ss CMF |
| **4. Contrefaçon intégrale** | • « *Skimming* » : | |
| | – Fabrication d'appareil de lecture et enregistrement de données magnétiques. | Néant |
| | – Détention de ces matériels avant la commission de l'infraction. | Néant |
| | – Captation des données magnétiques | art. 313-1 et ss CP |
| | • Contrefaçon intégrale d'un support : | |
| | – Fabrication de supports, reproduction des sécurités. | art. L. 163-4 et ss CMF |
| | – Encodage et embossage sur des supports contrefaits. | art. L. 163-4 et ss CMF |
| | – Usage des supports contrefaits réencodés et acceptation volontaire. | art. L. 163-4 et ss CMF |
| | – Détention du matériel ayant servi à la contrefaçon et à la fabrication. | art. L. 163-4 et ss CMF |
| | – Détention de supports contrefaits. | art. L. 163-4 et ss CMF |
| **5. Atteintes aux sécurités électroniques de la carte à puce** | – Analyse des flux électroniques entre la puce et le terminal de paiement. | art. 323-1 et ss CP et art. 323-2 et ss CP |
| | – Clonage de la puce et utilisation de la puce. | art. L. 163-4 et ss CMF |
| **6. Diffusion par tout moyen d'informations ou de données susceptibles de porter atteinte à la sécurité des moyens de paiement** | – Mise à disposition, détention de moyens de déclinaison de numéro (logiciels de moulinage…). | Néant |
| | – Diffusion et mise à disposition d'informations confidentielles sur les sécurités des moyens de paiement. | Néant |
| | – Mise à disposition et diffusion de méthodes de fraudes. | Néant |
| | – Vente, achat, transmission de ces matériels ou données. | Néant |
| | – Fabrication et élaboration de ces matériels ou génération de fausses données et mise à disposition sans infraction pour une fraude ultérieure. | Néant |

(a) Code pénal.

(b) Code monétaire et financier.

*Source : Ministère de la justice.*

Il apparaît ainsi que nombre d'actes concourant à la réalisation de la fraude ne peuvent, en l'état actuel de la législation, être réprimés, sauf s'ils sont directement reliés à une infraction constatée. Il convient de citer, à titre d'exemple, la fabrication, la détention, la mise à disposition de fausses façades de DAB, la récupération et la vente de numéros de cartes bancaires, qui ne peuvent être incriminées que si elles sont directement rattachées à une fraude avérée. De même, la mise en ligne sur Internet de logiciels de création de numéros de cartes bancaires, de décryptage de données sécurisées, ainsi que le piratage de fichiers clients de sociétés (contenant les coordonnées bancaires) échappent à la répression.

Les **articles 9 à 12** du présent projet de loi proposent de pallier cette carence.

L'article 9 constitue la principale innovation en la matière. Il crée un article L. 163-4-1 du code monétaire et financier, qui incrimine le fait « *de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou données conçus ou spécialement adaptés pour commettre les infractions prévues au 1° de l'article L. 163-3 et au 1° de l'article L. 163-4* » (qui prévoient l'incrimination des actes de contrefaçon et de falsification).

Ces infractions sont punies de sept ans d'emprisonnement et de 750.000 euros (4.919.677,50 francs) d'amende.

Conformément aux dispositions de l'article 121-4 du code pénal, l'article 9 précise également que la tentative du délit de l'article L. 163-4-1 du code monétaire et financier est punissable. Il étend, par ailleurs, la répression de la tentative aux falsifications et contrefaçons des moyens de paiement autres que les espèces.

L'article 10 complète les dispositions actuelles relatives à la confiscation et à la destruction des matériels, en y ajoutant les matériels mentionnés par le nouvel article L. 163-4-1 précité.

L'article 11 prévoit que les peines complémentaires applicables aux personnes physiques (privation pour cinq ans des droits civiques, civils et de famille) peuvent aussi être prononcées par le tribunal dans le cas d'une condamnation en application de l'article L. 163-4-1 précité.

Enfin, l'article 12 propose de créer un nouvel article L. 163-10-1 du code monétaire et financier, afin que les personnes morales puissent également être déclarées responsables pénalement des infractions relatives aux chèques et aux cartes de paiement. Dès lors, les personnes morales sont susceptibles des sanctions suivantes :

« *– 1° La dissolution, lorsque la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq ans, détournée de son objet pour commettre les faits incriminés ;*

*2° L'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;*

*3° Le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire ;*

*4° La fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;*

*5° L'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;*

*6° L'interdiction, à titre définitif ou pour une durée de cinq ans au plus, de faire appel public à l'épargne ;*

*7° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;*

*8° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;*

*9° L'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication audiovisuelle.*

*Les peines définies aux 1° et 3° ci-dessus ne sont pas applicables aux personnes morales de droit public dont la responsabilité pénale est susceptible d'être engagée. Elles ne sont pas non plus applicables aux partis ou groupements politiques ni aux syndicats professionnels. La peine définie au 1° n'est pas applicable aux institutions représentatives du personnel* » (article 131-39 du code pénal).

Dans le cas des infractions relatives aux chèques et aux cartes de paiement, il est précisé que l'interdiction mentionnée au 2° de l'article 131-39 du code pénal porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

En outre, les personnes morales encourent une amende dont le taux maximum est égal, en application de l'article 131-38 du code pénal, au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction. S'agissant des infractions relatives aux chèques et aux cartes de paiement, les personnes morales seraient donc susceptibles de se voir infliger des amendes allant jusqu'à 3.750.000 euros (24.598.387,50 francs).

Ces diverses dispositions peuvent faire l'objet de plusieurs remarques.

• **Les sanctions applicables en matière de monnaie scripturale sont sensiblement moins fortes que celles concernant la monnaie fiduciaire**

L'article 442-1 du code pénal prévoit, par exemple, que la contrefaçon ou la falsification de pièces de monnaie ou de billets de banque est punie de trente ans de réclusion criminelle et de 3 millions de francs d'amende, alors que la contrefaçon ou la falsification d'un chèque ou d'une carte de paiement peut certes donner lieu à une amende supérieure (5 millions de francs), mais à une peine d'emprisonnement sensiblement plus faible (sept ans d'emprisonnement).

Cette différence s'explique probablement par le fait que la fausse monnaie porte atteinte à un pouvoir régalien, tandis que les infractions relatives à la monnaie scripturale sont réprimées depuis peu de temps et concernent des moyens de paiement émis par des personnes privées.

• **Les infractions prévues par le présent projet de loi donnent déjà lieu à sanctions chez la plupart de nos partenaires**

Comme le montre le tableau suivant, les dispositions répressives déjà en vigueur ou proposées par le présent projet de loi se situent dans la moyenne de celles édictées par les Etats membres du G 7.

**SANCTIONS APPLICABLES DANS LES PAYS DU G 7**

| | Canada | Allemagne | Italie | Japon | Grande-Bretagne | Etats-Unis | France |
|---|---|---|---|---|---|---|---|
| Vol d'une carte de paiement | 10 ans | 5 ans et amende | 1 à 5 ans et amende | 10 ans | 10 ans et amende | 15 ans et amende | 3 ans et amende |
| Falsification ou contrefaçon | 10 ans | 10 ans | 1 à 5 ans et amende | - 3 mois à 5 ans pour une carte embossée<br>- 5 ans et amende si la fraude porte sur la piste | 10 ans et amende | 15 ans et amende (deux fois le montant du préjudice) | 7 ans et amende |
| Fabriquer, réparer, acheter ou vendre, exporter ou importer ou posséder des appareils, matériels, instruments en sachant qu'ils ont été utilisés ou adaptés ou destinés à contrefaire ou à falsifier des cartes de paiement | 10 ans | non | 1 à 5 ans et amende | non | 10 ans et amende | 15 ans et amende | 7 ans et amende (proposition du projet de loi) |

*Source : Ministère de la justice.*

**• Les nouvelles incriminations prévues par l'article 9 du présent projet de loi ne doivent porter atteinte ni à la liberté d'expression, ni à la simple détention de matériels en vente libre**

Il importe donc que seuls soient sanctionnés les faits qui traduisent en eux-mêmes une volonté délictuelle, ce qui signifie, en particulier, que le juge devra effectivement vérifier que les équipements, instruments, programmes informatiques ou données ont été conçus ou spécialement adaptés pour commettre les infractions.

La simple détention d'un instrument susceptible de lire une piste magnétique ne saurait, par exemple, être réprimée.

• **Si l'article L. 163-6 du code monétaire et financier prévoit que le tribunal peut interdire au condamné, pour une durée de cinq ans, d'émettre des chèques autres que ceux qui permettent exclusivement le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, le présent projet de loi ne prévoit pas une interdiction d'utiliser une carte de paiement à l'encontre d'une personne condamnée pour des infractions relatives à ce moyen de paiement**

Toutefois, les fraudeurs en ce domaine procèdent plutôt à la contrefaçon ou à la falsification d'une carte autre que celle qu'ils peuvent avoir et il n'apparaît pas indispensable d'ajouter une sanction à une liste déjà fournie.

• **Les dispositions pénales du code monétaire et financier ne s'appliquent qu'aux infractions relatives aux cartes de paiement et de retrait**

Il en résulte donc que les cartes ne répondant pas à la définition des cartes de paiement et de retrait donnée par l'article L. 132l du code monétaire et financier – c'est-à-dire, notamment, les cartes qui ne sont pas émises par un établissement de crédit (les cartes privatives, notion qui doit être entendue de manière restreinte, puisque, par exemple, les cartes Cetelem ou Cofinoga ne sont pas des cartes privatives) – ne sont pas concernées par ces dispositions pénales.

Le groupe de travail interministériel précité n'a pas jugé opportun d'étendre le champ d'application de ces dispositions aux infractions aux cartes privatives, dans la mesure où les dispositions pénales de droit commun (notamment le délit de faux en écritures privées, réprimé par l'article 441-1 du code pénal) permettent d'ores et déjà de sanctionner les fraudeurs.

En tout état de cause, les nouvelles incriminations prévues par le présent projet de loi devrait faciliter les poursuites et améliorer le taux d'élucidation de ce type d'affaires : actuellement 17% seulement sont élucidées, au lieu de 60% pour le reste des infractions financières [(1)].

*(1)* Le Monde*, 31 janvier 2001, page 10.*

## C.- PROTEGER LES CONSOMMATEURS : L'EXTENSION DE LA POSSIBILITE DE MISE EN OPPOSITION AUX CAS D'UTILISATION FRAUDULEUSE

Le second alinéa de l'article L. 132-2 du code monétaire et financier, actuellement en vigueur, prévoit qu'il ne peut être fait opposition au paiement par carte qu'en cas de perte ou de vol de la carte, de redressement ou de liquidation judiciaires du bénéficiaire.

Ces dispositions résultent de l'article 22 de la loi du 11 juillet 1985 portant diverses dispositions d'ordre économique et financier qui a, par ailleurs, posé le principe de l'irrévocabilité de l'ordre de paiement donné au moyen d'une carte.

L'**article 7** du présent projet de loi modifie cet article codifié, afin de prévoir que la mise en opposition est également possible en cas « *d'utilisation frauduleuse de la carte* ».

Il a déjà été indiqué, en effet, que de nouvelles formes de fraude peuvent avoir lieu sans que le titulaire de la carte en soit dépossédé, c'est-à-dire en l'absence de vol ou de perte.

Dans une telle situation, la victime de la fraude n'a pas aujourd'hui la possibilité juridique de faire opposition sur sa carte de paiement, qui ne peut donc pas figurer dans le fichier des cartes en opposition (OPPOTOTA), géré par le Groupement des cartes bancaires, consulté lors de chaque demande d'autorisation « en ligne ».

Lors de l'examen de la loi n° 91-1382 du 30 décembre 1991 précitée, notre collègue, M. Michel Suchod, avait déjà proposé un amendement étendant l'opposition à l'utilisation frauduleuse de la carte, qui prévoyait également que les sommes contestées seraient consignées. Cet amendement, adopté par la Commission des lois, n'avait finalement pas été retenu dans le texte définitif.

Depuis, l'évolution des technologies (en particulier, la possibilité d'effectuer des achats par Internet ou de recharger des cartes prépayées de téléphonie mobile) et des techniques de fraude (la « *white plastic* » notamment) a rendu plus pressante la nécessité d'une extension de la faculté d'opposition.

Le texte proposé répond à cette nécessité. Il peut, néanmoins, faire l'objet de deux remarques.

• **La référence à l'utilisation frauduleuse de la carte** est parfois considérée comme étant trop restrictive et empêcherait – selon les tenants de cette interprétation – de faire opposition dans toutes les hypothèses où le titulaire de la carte, victime de la fraude, serait pourtant en possession de sa carte. Dès lors, il a été proposé de prévoir une extension de l'opposition aux cas d'utilisation frauduleuse « *du numéro* » de la carte.

Votre Rapporteur pour avis estime que cette nouvelle rédaction serait également susceptible d'une interprétation restrictive. Elle répondrait parfaitement aux fraudes constatées dans le cadre des paiements à distance, mais qu'en serait-il, par exemple, de la fraude à la « *white plastic* » où le fraudeur utilise toutes les données figurant sur la piste magnétique (entre autres le numéro de la carte, mais pas seulement) et le code secret qu'il a pu se procurer, éventuellement, par des moyens informatiques.

En conséquence, il apparaît souhaitable de s'en tenir à la rédaction proposée par le présent projet de loi, tout en précisant que par « utilisation frauduleuse de la carte », on entend toute utilisation, à l'insu de son titulaire, alors que ce dernier est en possession de sa carte.

• **Il convient également de préciser que cette nouvelle faculté de mise en opposition ne doit pas conduire à faire supporter la responsabilité financière de la fraude, intervenue avant la mise en opposition pour utilisation frauduleuse de la carte, par le titulaire de la carte.**

Actuellement, un titulaire dont la carte est perdue ou a été volée est responsable des pertes subies jusqu'à la mise en opposition (dans la limite généralement d'une franchise définie contractuellement), sur la base d'une « présomption conventionnelle de négligence ».

Dans le cadre d'une utilisation frauduleuse de la carte, cette présomption ne saurait être retenue, puisque le titulaire de la carte, victime de la fraude, n'a pas été dépossédé de sa carte et que les éléments ayant permis la fraude ont pu être interceptés sans même qu'il ait la possibilité de s'en rendre compte (piratage du numéro lors de sa transmission sur Internet ou copie de la piste magnétique grâce à un TPE modifié, par exemple).

On peut noter d'ailleurs que, dans un jugement récent du 23 novembre 2000, le tribunal d'instance de Paris a condamné la Société générale à rembourser à la titulaire d'une carte, ni perdue ni volée, la totalité des sommes débitées au titre de retraits que la titulaire n'avait pu effectuer. Dans le cas d'espèce, le montant total des retraits (5.000 francs) réalisés dans la même journée excédait le plafond contractuel (3.000 francs), ce qui

a suffi au tribunal à prouver l'existence d'un « *dysfonctionnement imputable à la Société générale* ».

Votre Rapporteur pour avis réaffirme cependant que, quelles que soient les circonstances de la fraude [(1)], aucune responsabilité financière ne saurait peser sur la personne victime d'une utilisation frauduleuse de sa carte, même avant qu'elle ait pu faire opposition. La recommandation de la Commission européenne 97/489/CE du 30 juillet 1997 pose d'ailleurs clairement ce principe dans le point 3 de son article 6 : « *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). La seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire* ».

De la même façon, en cas d'utilisation frauduleuse de la carte, il ne saurait être accepté que le titulaire qui a tardé à faire opposition soit considéré comme fautif. Un tel principe, qui est retenu dans les hypothèses de vol ou de perte (Chambre commerciale de la Cour de cassation, 1er mars 1994), ne peut valoir dans le cas de l'utilisation frauduleuse, plus difficile et plus longue à détecter par la victime. Dans le cas contraire, comment pourrait-on d'ailleurs apprécier le caractère tardif de l'opposition ? Faudrait-il prendre pour point de départ la date de réalisation de l'opération frauduleuse, celle de la réception par le titulaire du relevé bancaire mentionnant cette opération, ou encore la date où cette opération a figuré sur le site Internet de la banque ?

En tout état de cause, il convient de rappeler qu'aux termes de l'article 13 du « contrat porteur " CB " » version 7 (la dernière version), le titulaire de la carte ne peut déposer une réclamation que dans un délai de 120 jours maximum (parfois moins, comme cela sera indiqué ci-dessous).

Les dispositions du présent projet de loi relatives aux cartes de paiement étaient attendues et leur efficacité devrait être renforcée par la mise en œuvre des engagements souscrits par les professions concernées le 22 février dernier et par les nombreuses initiatives internationales en ce domaine.

---

*(1) A cet égard, il est appréciable que les banques se soient engagées, dans la charte signée le 22 février 2001, à préciser dans le contrat « porteur » que les enregistrements des DAB ne constituent pas la seule preuve de la transaction.*

## II.- UN DISPOSITIF COMPLETE PAR DES ENGAGEMENTS DES PROFESSIONNELS ET DES INITIATIVES INTERNATIONALES

A la suite de la remise du rapport réalisé dans le cadre du Conseil national de la consommation, le Gouvernement a annoncé les mesures d'ordre législatif, précédemment étudiées, ainsi que son intention de donner une impulsion nouvelle aux groupes européens de concertation agissant dans le cadre de l'initiative « *e*-Europe ».

Le jour même de cette annonce, le 22 février 2001, deux chartes relatives à la sécurité des cartes de paiement étaient signées respectivement par les banques et par le Conseil du commerce de France.

Dans le cadre du présent avis, votre Rapporteur se bornera à quelques commentaires sur ces engagements et ces initiatives internationales, qui donneront lieu à un examen plus détaillé dans le rapport d'information dont il est également chargé.

### A.- LES ENGAGEMENTS DES PROFESSIONNELS

Les professions concernées (et le Gouvernement, pour ce qui relève de la compétence de l'Etat) ont su répondre à la majeure partie des recommandations du rapport rédigé dans le cadre du Conseil national de la consommation. Le tableau comparatif suivant montre ainsi que 28 des 38 recommandations du groupe de travail ont été satisfaites (au moins partiellement).

**REPONSES AUX RECOMMANDATIONS**
**DU CONSEIL NATIONAL DE LA CONSOMMATION**

| Recommandations du Conseil national de la consommation | Mesures annoncées le 22 février 2001 |
|---|---|
| **● Aux établissements de crédits et émetteurs de cartes** | |
| – Mieux informer les porteurs : | |
| 1) lors de la signature d'un contrat | avant juillet 2001 |
| 2) sur les plafonds d'achats et de retraits | avant juillet 2001 |
| 3) sur le numéro unique d'opposition | avant juillet 2001 |
| 4) sur la formalisation de la contestation d'un débit à caractère frauduleux | |
| 5) sur l'existence, le cas échéant, d'un service de détection des utilisations anormales des cartes | |
| 6) mieux informer les commerçants sur les règles de recréditation du porteur dans le cadre de la vente à distance | avant juillet 2001 |
| – Sécuriser les retraits DAB | |
| 7) généralisation de la lecture de la puce | achèvement avant juillet 2001 |
| 8) espace de confidentialité | à moyen terme |
| 9) dispositif de mise en opposition depuis les DAB | |
| 10) réflexion sur l'ergonomie et les lieux d'installation | à moyen terme |
| 11) suppression des fonctions paiement et retrait de la piste sur les cartes nationales | à moyen terme |
| – Sécuriser les achats à distance | |
| 12) généraliser le cryptogramme visuel au verso | à moyen terme |
| 13) mettre en place un système de données permettant aux commerçants d'authentifier le lien entre porteur et payeur | à moyen terme |
| 14) mettre en place des fichiers incidents | |
| 15) favoriser la gestion de listes de cartes émises | |
| 16) accélérer le traitement des incidents | |

| Recommandations du Conseil national de la consommation | Mesures annoncées le 22 février 2001 |
|---|---|
| | [*Charte du 22 février 2001 : déployer des solutions techniques de paiement sécurisé en ligne visant à supprimer la circulation des numéros en ligne (à moyen terme).]* (1) |
| – Améliorer les règles de fonctionnement | |
| 17) mise en opposition sans communication du numéro | avant juillet 2001 |
| 18) informer les porteurs sur la conduite à tenir en cas de capture de la carte par un DAB | avant juillet 2001 |
| 19) transmettre aux porteurs les versions actualisées des contrats | |
| 20) permettre aux titulaires de cartes de lire la puce | La charte du 22 février 2001 s'engage sur la poursuite des travaux sur ce point (à moyen terme) |
| 21) mettre en œuvre un processus d'activation de la carte après réception et à l'initiative du porteur | à moyen terme |
| | *[Charte du 22 février 2001* : *élargir le choix des tranches de plafonds d'achats et de retraits (à moyen terme)]* |
| – Revoir le partage de la responsabilité financière | |
| 22) rembourser l'ensemble des frais subis par le porteur en cas d'utilisation frauduleuse (hors vol ou perte) | avant juillet 2001 |
| 23) rembourser dans le délai maximum d'un mois les débits frauduleux | avant juillet 2001 |
| 24) limiter la franchise (en cas de perte ou vol) à 150 euros | franchise de 400 euros |
| 25) mettre en conformité le contrat porteur avec les recommandations de la Commission des clauses abusives (en précisant que les enregistrements des DAB constituent des preuves simples susceptibles d'être contestées par tous moyens, d'une part, et que l'émetteur ne limite pas sa responsabilité, en cas de mauvais fonctionnement du système au seul préjudice direct subi par le porteur, d'autre part) | La charte du 22 février 2001 s'engage à préciser que les enregistrements des DAB ne constituent pas la seule preuve de la transaction |
| 26) inscrire, dans le contrat porteur, le droit de se faire recréditer en cas d'utilisation frauduleuse sans usage du code | avant juillet 2001 |

*(1) Les mesures figurant en italiques correspondent à des dispositions ne répondant pas directement à l'une des recommandations du Conseil national de la consommation.*

| Recommandations du Conseil national de la consommation | Mesures annoncées le 22 février 2001 |
|---|---|
| **● Au secteur du commerce de proximité et de la grande distribution** | |
| 27) garantir la confidentialité de la frappe du code | Charte du Conseil du commerce de France du 22 février 2001 : avant fin 2001 |
| 28) supprimer les numéros de carte complets et l'identité sur les facturettes | Charte du Conseil du commerce de France du 22 février 2001 : avant fin 2001 |
| **● Au secteur du commerce de la vente à distance** | |
| 29) informer sur les techniques de sécurisation de paiement mises en œuvre | Charte du Conseil de commerce de France du 22 février 2001 |
| 30) ne pas stocker dans des bases de données des informations relatives aux numéros de cartes et de cryptogrammes visuels | |
| 31) déployer des solutions techniques pour sécuriser le paiement en ligne | [Un engagement a été pris dans la charte signée par les banques, mais ne figure pas dans celle signée par le Conseil du commerce de France] |
| **● Aux opérateurs de téléphonie mobile** | |
| 32) mise en œuvre de mesures d'encadrement (un seul numéro de carte par carte prépayée, limitation du montant du rechargement…) | [Annoncé par le Gouvernement, mais ne figure pas dans les chartes signées] |
| 33) généraliser le cryptogramme visuel | à moyen terme |
| **● Aux pouvoirs publics** | |
| 34) aggraver les peines liées à l'intrusion dans les systèmes monétiques et à la diffusion d'informations sur la contrefaçon des cartes | Projet de loi sur la sécurité quotidienne |
| 35) mieux réprimer les agissements facilitant la fraude sur Internet | Projet de loi sur la sécurité quotidienne |
| 36) impliquer davantage la Banque de France | Projet de loi sur la sécurité quotidienne |
| 37) conférer à la Mission « économie numérique », une mission de veille sur les paiements en ligne et la cyber-criminalité | |
| 38) réunir le Conseil national de la consommation au second semestre pour faire le point | |
| | [*Étendre l'opposition au cas de fraude (projet de loi)*] |
| | [*Observatoire de la sécurité des cartes bancaires ayant pour mission notamment de suivre la mise en œuvre de la charte du 22 février 2001*] |
| | [*Impulsion aux groupes européens de concertation pour établir, notamment, des normes européennes de paiement sécurisé*] |

Les engagements souscrits par les banques et par le secteur du commerce constituent une avancée significative, notamment dans les domaines de :

- **la sécurité**

Les professionnels ont ainsi décidé de :

– généraliser la lecture de la puce par les DAB ;

– supprimer les fonctions paiement et retrait de la piste sur les cartes bancaires nationales (1) ;

– généraliser le cryptogramme visuel au verso de la carte ;

– tronquer le numéro et l'identité du porteur sur les facturettes.

- **la protection des consommateurs**

Il est prévu, notamment :

– d'inscrire dans le contrat porteur le droit du titulaire de carte 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, en rappelant les sanctions pénales liées aux fausses déclarations ;

– de 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.

Il convient également d'observer que certaines mesures annoncées le 22 février dernier par les professionnels ne correspondent à aucune des recommandations expressément formulées par le groupe de travail du Conseil national de la consommation. Ces mesures viennent donc compléter utilement le dispositif. Elles visent à déployer des solutions techniques de paiement sécurisé en ligne et à élargir le choix des tranches de plafonds d'achats et de retraits.

Toutefois, les deux chartes signées le 22 février 2001 peuvent aussi faire l'objet de plusieurs réserves.

---

*(1) La piste magnétique ne peut être entièrement supprimée, ne serait-ce que pour ouvrir les sas permettant d'accéder aux DAB protégés par une enceinte. En outre, pour les cartes internationales (la majeure partie des cartes bancaires en circulation), elle doit être maintenue car, à l'étranger, peu de DAB et de TPE lisent la puce.*

• **Des propositions du rapport rédigé dans le cadre du Conseil national de la consommation n'ont pas été reprises**

Aucun engagement, figurant dans les deux chartes signées, ne prévoit, par exemple :

– d'informer les porteurs sur l'existence, le cas échéant, d'un service de détection des utilisations anormales des cartes ;

– de favoriser la mise en place des fichiers incidents au niveau professionnel en matière d'achats à distance ;

– d'accélérer le traitement des incidents par les banques ;

– de transmettre aux titulaires de cartes un contrat actualisé et conforme à la dernière version adoptée par le Groupement des cartes bancaires.

La transparence dans les relations banques-clients ne s'en trouve pas renforcée. A cet égard, il est significatif que la recommandation visant à mettre en conformité les contrats porteurs avec une recommandation faite, en 1991, par la Commission des clauses abusives, n'ait pas été retenue. Les banques refusent donc de préciser que l'émetteur de la carte ne limite pas sa responsabilité, en cas de mauvais fonctionnement du système, au seul préjudice direct subi par le porteur.

• **Des engagements répondant partiellement aux recommandations**

Le groupe de travail du Conseil national de la consommation souhaite que l'on permette au titulaire d'une carte de lire la puce de sa carte, afin de disposer de la liste des opérations effectuées (le « talon » électronique). Cette fonctionnalité peut actuellement être mise en œuvre, mais il n'est pas encore certain qu'elle sera maintenue dans le cadre de la nouvelle norme internationale EMV. Or, la charte signée par les professions bancaires les engage seulement à « *poursuivre les travaux visant à permettre l'inscription dans la puce de toutes les opérations effectuées et leur lecture par le titulaire de la carte* ». Néanmoins, selon les informations fournies à votre Rapporteur pour avis, les cartes du GIE « CB » devraient effectivement maintenir, à titre obligatoire, cette fonctionnalité. Il serait maintenant souhaitable de procéder aux adaptations permettant une identification précise du bénéficiaire du paiement, voire de faire figurer dans les talons, les retraits opérés sur les DAB.

Un autre point – plus important encore – n'est satisfait que très partiellement par les engagements pris le 22 février dernier. Il s'agit du problème de la franchise laissée à la charge des porteurs pour ce qui concerne la fraude antérieure à la déclaration de perte ou de vol. Conformément aux recommandations de la Commission européenne du 17 novembre 1988 et du 30 juillet 1997, le groupe de travail du Conseil national de la consommation a souhaité que cette franchise soit limitée à 150 euros. La charte du 22 février la porte à 400 euros. Cela constitue déjà une avancée, mais le ministre de l'économie, des finances et de l'industrie a lui même reconnu qu'« *il faudra parvenir dans le futur à un résultat encore meilleur* ».

S'agissant toujours du problème de la franchise, il convient de remarquer que les banques n'acceptent de l'appliquer que si le porteur a fait opposition dans les 24 heures, délai paraissant trop bref.

• **Des mesures correspondant à des annonces préalablement effectuées et ayant subi des retards de mise en œuvre**

Plusieurs des engagements souscrits le 22 février dernier par les professions bancaires et par le Conseil du commerce de France ne sont, en fait, que la reprise de mesures déjà annoncées par le passé et qui n'ont pas été mises en application dans les délais prévus.

Il en est ainsi de la promesse d'achever la modernisation de tous les DAB avant le 1er juillet 2001, afin de garantir la lecture des puces des cartes. Le Groupement des cartes bancaires s'était déjà engagé par le passé à achever cette modernisation fin 2000. Or, à cette date, 33% des DAB n'étaient toujours pas en mesure de lire la puce.

De même, la suppression de certaines données (numéro, identité) sur les facturettes, a déjà été annoncée à plusieurs reprises, notamment à la suite de la Table ronde organisée en avril 2000 (1).

Enfin, les banques avaient mis en place un « code de bonne conduite » pour régler les litiges les plus fréquents, par lequel elles décidaient de rembourser dans les huit jours qui suivent la plainte (et dans les deux mois, s'il s'agit d'un litige à l'étranger), les litiges les plus

---

*(1) On peut observer que certains états des Etats-Unis ont décidé d'imposer cette mesure par la loi. La Californie a en effet interdit, à partir du 1er janvier 2001, pour les terminaux nouvellement installés chez les détaillants, l'impression des premiers chiffres du numéro de compte d'un titulaire de carte bancaire sur son reçu. Cette même loi requiert que les terminaux imprimant le numéro de compte en entier ne soient plus utilisés à partir du 1er janvier 2004. La date d'expiration de la carte sera également supprimée. Dans l'Etat de Washington, une loi aux dispositions similaires entrera en vigueur le 1er juin 2001 et s'appliquera à l'ensemble des terminaux au 1er juin 2004.*

fréquents (« *white plastic* » et Internet) dans lesquels la bonne foi du porteur est évidente. Dès lors, l'engagement pris, dans la Charte du 22 février dernier, de rembourser en moins d'un mois les débits frauduleux peut, dans certains cas, apparaître en retrait par rapport au code de bonne conduite.

- **Des mesures à préciser**

Certains engagements souscrits par les professionnels mériteraient d'être précisés.

On peut, tout d'abord, noter que si la charte signée par les banquiers contient des engagements, celle signée par le Conseil du commerce de France n'impose à ce dernier que des recommandations à ses adhérents.

Par ailleurs, il serait souhaitable que les banques indiquent expressément ce qu'elles entendent par remboursement des « frais bancaires », subis en cas de fraude liée à l'utilisation d'un numéro de carte ou d'une carte contrefaite. Il conviendrait d'être sûr, en effet, que ces termes recouvrent bien ce qui est demandé par le groupe de travail, à savoir le montant des transactions, les agios le cas échéant, les frais de mise en opposition et ceux de renouvellement de la carte.

Enfin, il importe de souligner qu'aucun engagement n'a été pris en ce qui concerne la mise à niveau régulière de la sécurité de la puce. Or, il est notoire que l'affaire Humpich n'aurait pas eu lieu si le Groupement des cartes bancaires avait tenu compte des conseils donnés, dès 1988, par certains spécialistes et avait procédé notamment au rallongement des clés secrètes. On peut supposer, néanmoins, que, lorsque le présent projet de loi prévoit que « *la Banque de France s'assure de la sécurité des instruments de paiement et de la pertinence des normes applicables en la matière* », il sous-entend que ladite institution devra veiller à la maintenance de la sécurité de la puce (le groupe de travail technique précise d'ailleurs qu'un mécanisme de maintenance est prévu dans le cadre du schéma national d'évaluation et de certification). Il serait, toutefois, opportun d'obtenir confirmation de cette interprétation et de veiller, en outre, à la maintenance de la sécurité des TPE.

- **Des engagements qui ne recouvrent qu'une partie des mesures de sécurisation décidées par les professionnels.**

Les engagements pris le 22 février confortent des actions décidées précédemment.

– Par un accord, conclu le 17 janvier 2001, les établissement bancaires membres du Groupement des cartes bancaires et les accepteurs de cartes, représentés par le Conseil du commerce de France, ont prévu les modalités de modernisation de l'ensemble du parc des terminaux de paiement électronique vers le programme CB 5.

Ce programme prend en compte les grandes évolutions nationales et internationales du paiement par cartes bancaires : le passage à l'euro, l'amélioration de la sécurité, la compatibilité au standard international EMV, ainsi que les applications commerciales autres que le paiement (programmes de fidélité par exemple).

La migration des terminaux de paiement électronique de l'ensemble du commerce vers le programme CB 5 devra être terminée le 1er mai 2003. Une première étape, déjà engagée par la moitié du commerce de proximité, s'achèvera avant la fin 2001 pour renforcer le niveau de sécurité des équipements et assurer le passage à l'euro. Au terme de ce processus, près d'un million de commerçants seront équipés. Plus de cinq milliards de francs seront investis conjointement par le commerce et les banques « CB ».

– Le 20 février 2001, un accord a également été signé entre le GIE cartes bancaires et les professions de la vente à distance et du commerce en ligne, afin de redonner confiance aux porteurs de cartes en améliorant la sécurité du « *e*-commerce ».

Dans cet accord, les différents signataires ont pris divers engagements.

L'Association des fournisseurs d'accès (AFA) a affirmé développer une déontologie forte, notamment en matière de données personnelles et de traitement des réclamations, pour permettre de conserver la confiance des internautes dans leur accès à Internet.

La Fédération des entreprises de vente à distance (FEVAD) a souhaité intensifier la promotion du sceau L@belsite, référentiel de qualité pour les sites marchands, qui garantit l'identité des commerçants, la clarté de l'information commerciale, la transparence des données à caractère personnel et nécessite un moyen de sécurisation des transactions.

Le Groupement des cartes bancaires « CB » s'est engagé à développer les solutions de télépaiement sécurisé par carte à puce : lecteurs

de type Cyber-comm (en voie d'homologation européenne « *Finread* »), paiement CB sur téléphone mobile… [(1)].

Les problèmes rencontrés par le boîtier Cyber-comm seront évoqués dans le futur rapport d'information. Néanmoins, votre Rapporteur pour avis se demande si sa diffusion ne pourrait pas être facilitée grâce à une distribution gratuite, par les banques, auprès des consommateurs intéressés. A cet égard, il est intéressant de noter qu'aux Etats-Unis, American Express a distribué gratuitement jusqu'au 31 janvier 2000 [(2)] un lecteur permettant à sa carte « *Blue* » d'être dotée de fonctions de porte-monnaie électronique dans des conditions de sécurité renforcée.

– Enfin, il convient de rappeler plusieurs programmes mis en œuvre par le GIE carte bancaires.

A l'automne 2001, toutes les cartes « CB » en circulation seront équipées de clés secrètes allongées (768 bits).

De même, à compter du second semestre 2002, le réseau téléinformatique interbancaire de transport d'autorisations sera modernisé pour permettre de faire face à la croissance attendue du nombre d'autorisations, pour renforcer la sécurité et pour offrir aux banques la possibilité de transporter des informations associées à de nouveaux services. Ce nouveau réseau est appelé RSB (Réseau de Service aux Banques).

## B.- DE MULTIPLES INITIATIVES COMMUNAUTAIRES ET INTERNATIONALES

Dans une communication du 9 février dernier, la Commission européenne observe que le volume de la fraude transfrontalière est supérieur à celui de la fraude nationale. Il est donc compréhensible que les instances communautaires et internationales se mobilisent, d'une façon quelque peu foisonnante.

---

*(1) D'une façon plus générale, la sécurisation de la vente à distance devrait être facilitée par la décision prise par le Gouvernement lors du comité interministériel pour la sécurité de l'information du 19 janvier 1999, d'offrir une liberté totale dans l'utilisation de la cryptologie et de supprimer, en conséquence, toute limitation tenant à la taille des clés employées, ainsi que les contraintes pesant actuellement sur la gestion de ces clés par un « tiers de séquestre ». Une première étape a été franchie, en mars 1999, lorsque le seuil de la cryptologie, dont l'utilisation est libre, a été relevé par décret de 40 à 128 bits. Une seconde étape, d'ordre législatif, devrait être prévue dans le projet de loi relatif à la société de l'information, dont le dépôt pourrait intervenir prochainement. Ce projet de loi devrait accompagner cette libéralisation d'une politique de sécurité, se traduisant, notamment, par le renforcement des pouvoirs d'accès des autorités judiciaires à une version « en clair» des données chiffrées.*

*(2) Depuis cette date, le lecteur est vendu au prix de 25 dollars.*

## 1.- A l'échelon communautaire

• La Commission européenne a adopté le 1er juillet 1998 une communication intitulée : « *Un cadre d'action pour lutter contre la fraude et la contrefaçon des moyens de paiement autres que les espèces* ».

• Sur cette base, une décision-cadre du Conseil a été élaborée avec pour objectif essentiel de faire en sorte que toute fraude impliquant un moyen de paiement autre que les espèces soit érigée en infraction pénale et que des mécanismes de coopération adéquats soient mis en place, afin que les auteurs de ces infractions soient effectivement poursuivis.

• La décision-cadre est complétée par une communication de la Commission du 9 février 2001, qui invite le Conseil et le Parlement européen à adopter un plan d'action pour la prévention de la fraude sur les cartes de paiement, qui aurait atteint 600 millions d'euros dans l'Union européenne (soit 0,07% du chiffre d'affaires du secteur des cartes de paiement).

Ce plan prévoit notamment :

– l'introduction d'un numéro de téléphone unique opérationnel dans tous les Etats membres (ou du moins un numéro de téléphone unique permettant de joindre tous les émetteurs établis dans chaque Etat membre) pour faciliter la notification par les consommateurs de la perte ou du vol de leurs cartes ;

– la publication par la Commission, en concertation avec les autorités nationales chargées de la protection des données, de lignes directrices sur les critères à respecter pour les échanges d'informations relatives à la prévention de la fraude ;

– le lancement d'une « *page* web *de prévention de la fraude* » contenant des information sur les initiatives en matière de prévention de la fraude et proposant des liens vers tous les organismes compétents ;

– l'adoption d'initiatives ciblées visant à améliorer la sécurité des produits et des systèmes de paiement, sur la base des résultats d'une étude de la Commission sur certains aspects spécifiques de la sécurité ;

– l'encouragement des représentants du secteur des systèmes de paiement et des services de répression à définir les éléments de preuve qu'ils jugent indispensables pour ouvrir une enquête et engager des poursuites dans les affaires de fraude et à convenir des modalités d'échange des informations pertinentes.

• Dans le cadre de l'initiative *e*-Europe 2002, un « sommet de la carte à puce » s'est déroulé à Lisbonne, le 11 avril 2000, et une charte de la carte à puce a été adoptée afin de soutenir des démarches communes concernant le déploiement des cartes à puce dans l'Union européenne.

## 2.- Au niveau international

• Un projet de convention sur la cyber-criminalité est examiné dans le cadre du Conseil de l'Europe afin, notamment, de renforcer la coopération internationale (en particulier, en ce qui concerne les investigations et les extraditions). La Commission des questions juridiques et des droits de l'Homme de l'Assemblée parlementaire du Conseil de l'Europe a procédé à des auditions, le 6 mars dernier, dans les locaux de l'Assemblée nationale.

• Le G 8 examine les questions liées à la cyber-criminalité depuis 1997. Des rencontres régulières entre des représentants des services répressifs et des industriels ont été organisées.

## CHAPITRE IV

## UN DISPOSITIF SUSCEPTIBLE D'ETRE COMPLETE

Il a déjà été signalé que, lors de son intervention du 22 février dernier annonçant les mesures législatives figurant dans le présent projet de loi et précédant la signature de deux chartes relatives à la sécurité des cartes de paiement, M. le ministre de l'économie, des finances et de l'industrie a clairement mentionné qu'« *il s'agi*[ssait] *d'un premier train de mesures. Il a vocation à être prolongé dans le cadre de discussions en cours et à venir avec l'ensemble des parties prenantes, en particulier les associations de consommateurs* ».

Pour s'en tenir aux mesures d'ordre législatif, votre Rapporteur pour avis considère qu'il est possible, dès à présent, de compléter le dispositif proposé, en prévoyant, d'une part, de conforter les compétences de la Banque de France et, d'autre part, de renforcer la protection des consommateurs.

### I.- CONFORTER LES COMPETENCES DE LA BANQUE DE FRANCE

Les dispositions prévues par l'article 8 du présent projet de loi (et par l'article 16, en ce qui concerne l'Institut d'émission d'outre-mer) ont été présentées au chapitre précédent. Elles donnent expressément compétence à la Banque de France pour s'assurer de la sécurité des moyens de paiement, ce qui devrait, en particulier, accroître son rôle au sein du conseil de direction du GIE cartes bancaires, où elle siège en qualité d'observateur [(1)]. Elles lui attribuent, par ailleurs, la capacité de vérifier la pertinence des normes applicables, grâce à des expertises et à la communication des informations utiles. Enfin, ces dispositions permettent à la Banque de France de formuler un avis négatif à l'encontre d'un moyen de paiement dont elle estimerait qu'il présente des garanties de sécurité insuffisantes.

Votre Rapporteur pour avis approuve ces mesures, mais il estime qu'elles méritent d'être précisées, tant en ce qui concerne la capacité de contrainte reconnue à la Banque de France, qu'en ce qui concerne le champ de ses investigations. Il souhaiterait, en outre, lui confier des responsabilités

*(1) Il convient de noter qu'après la promulgation du présent projet de loi, la Banque de France restera « observateur », mais les autres membres sauront désormais qu'elle dispose de moyens pour imposer son point de vue et devraient donc être plus réceptifs à ses interventions.*

au sein de deux nouveaux organismes, l'Observatoire de la sécurité des cartes bancaires (dont la création a été annoncée par le Gouvernement) et le Comité de veille technologique pour les systèmes de paiement, dont les travaux aideraient la banque centrale à s'assurer de la sécurité des moyens de paiement.

### A.- UN VERITABLE POUVOIR D'OPPOSITION A L'ENCONTRE DES MOYENS DE PAIEMENT INSUFFISAMMENT SECURISES

Le texte proposé prévoit que la Banque de France peut recommander à l'émetteur d'un moyen de paiement de prendre toutes mesures destinées à remédier aux insuffisances constatées et, si ces recommandations n'ont pas été suivies d'effet, elle peut décider de formuler un avis négatif et de le rendre public.

#### 1.- La publicité de l'avis négatif doit être obligatoire et formalisée

La possibilité de rendre publics les avis négatifs formulés par la Banque de France sur la sécurité d'un moyen de paiement constitue l'une des principales innovations prévues par l'article 8 du présent projet de loi, puisque la banque centrale a d'ores et déjà la faculté de présenter des recommandations dans le cadre de son rôle d'observateur au sein du conseil de direction du GIE des cartes bancaires.

Pourtant, la rédaction actuelle du texte peut laisser supposer que la Banque de France pourra choisir de ne pas rendre publics de tels avis, alors même qu'une recommandation formulée précédemment sans aucune publicité serait restée lettre morte.

Il serait donc opportun de rendre obligatoire leur publication et de la formaliser en prévoyant qu'elle aura lieu au *Journal officiel*.

#### 2.- La Banque de France doit être dotée d'un véritable pouvoir d'opposition

Lors de son intervention du 22 février dernier, le ministre de l'économie, des finances et de l'industrie a affirmé que la Banque de France disposerait désormais « *du pouvoir de s'opposer à la mise à disposition du public de toute carte de paiement dont les fonctions de sécurité seraient insuffisantes* ».

Or, formellement, le texte proposé ne lui donne pas un tel pouvoir.

Certes, il y a tout lieu de penser qu'un avis négatif rendu public nuirait gravement à l'usage du moyen de paiement concerné et équivaudrait, en fait, à un pouvoir d'opposition.

Néanmoins, en droit, rien n'empêcherait la poursuite de l'émission dudit moyen de paiement et la circulation, par exemple, des cartes de paiement déjà émises dont la sécurité est contestée.

Il serait donc nécessaire de prévoir que tout moyen de paiement ayant fait l'objet d'un avis négatif ne peut être émis et circuler tant que son émetteur ne s'est pas conformé aux recommandations de la Banque de France. En outre, par symétrie des formes, il conviendrait d'indiquer que cette opposition ne pourrait être levée que par la publication, au *Journal officiel*, d'un avis positif.

### B.- DES CAPACITES D'EXPERTISES ET DE COMMUNICATION D'INFORMATIONS ETENDUES AUX TERMINAUX OU AUX DISPOSITIFS TECHNIQUES ASSOCIES AUX MOYENS DE PAIEMENT

L'article 8 du présent projet de loi prévoit que, pour s'assurer de la sécurité des moyens de paiement et de la pertinence des normes applicables, la Banque de France procède aux expertises et se fait communiquer les informations utiles.

Dans le cas spécifique des cartes de paiement, il va de soi que ces attributions permettront de s'assurer de la sécurité de la puce.

Des évaluations de cette sécurité sont déjà mises en œuvre dans le cadre du schéma français d'évaluation et de certification institué par la direction centrale de la sécurité des systèmes d'information (DCSSI). Elles sont réalisées par les centres d'évaluation de la sécurité des technologies d'information (CESTI).

Toutefois, l'importance des terminaux dans la sécurité des cartes à puce a déjà été soulignée, dans la mesure où ces matériels représentent un maillon faible de la chaîne sécuritaire. Le rapport du groupe technique restreint considère d'ailleurs que « *les terminaux, au même titre que la puce, pourraient être soumis à une évaluation de sécurité conformément au schéma national associé à un programme de maintenance* ».

Dès lors, il importe d'étendre expressément les compétences de la Banque de France, en matière d'expertises et de communication d'informations, aux terminaux ou aux dispositifs techniques associés aux moyens de paiement.

## C.- DEUX NOUVEAUX ORGANISMES ASSISTANT LA BANQUE DE FRANCE

### 1.- L'Observatoire de la sécurité des cartes bancaires

Le Gouvernement a annoncé, le 22 février dernier, la prochaine mise en place d'un Observatoire de la sécurité des cartes bancaires, en précisant uniquement qu'il serait chargé de suivre la mise en œuvre des engagements souscrits, le même jour, par les professionnels, dans deux chartes.

Deux mois après cette annonce, ledit Observatoire n'a toujours pas été institué, alors même que nombre des engagements figurant dans les deux chartes doivent être mis en œuvre à court terme (avant le 1er juillet 2001).

Il apparaît donc nécessaire de créer cet organisme par voie législative.

Il serait ainsi possible, en outre, de préciser sa composition et ses missions, qui pourraient aller au-delà de ce que le Gouvernement a envisagé.

Etant conçu comme une instance de dialogue, l'Observatoire devrait regrouper les différents acteurs concernés : administrations, émetteurs de cartes de paiement, représentants des porteurs et des commerçants. Sa présidence serait assurée par la Banque de France et son secrétariat par l'un des représentants des associations de consommateurs.

Du fait de sa composition élargie, l'Observatoire pourrait se voir confier, outre la surveillance et l'évaluation de la mise en œuvre des deux chartes du 22 février et d'éventuelles mesures de sécurisation entreprises par les émetteurs, l'établissement de statistiques de la fraude. Ces dernières, contrairement à celles fournies par le GIE cartes bancaires, prendraient en compte l'ensemble des cartes de paiement et de retrait (et pas seulement les cartes « CB ») et ne se borneraient pas à recenser la fraude supportée par les établissements de crédit et les banques.

### 2.- Le Comité de veille technologique pour les systèmes de paiement

Parmi les recommandations adressées aux pouvoirs publics par le rapport réalisé dans le cadre du Conseil national de la consommation, figure une proposition visant à confier à la mission « économie numérique » du ministère de l'économie, des finances et de l'industrie, en association avec

le ministère de l'intérieur et le ministère de la justice, une mission de veille sur la sécurité des paiements en ligne et sur la cyber-criminalité.

Il serait donc souhaitable de prévoir, dès à présent, la création de ce Comité de veille technologique, dont le secrétariat serait attribué à la Banque de France, compte tenu des compétences que l'article L. 1414 du code monétaire et financier lui donne en matière de fonctionnement et de sécurité des systèmes de paiement.

Ce comité, de composition beaucoup plus restreinte que l'Observatoire précité, permettrait aux administrations chargées de la lutte contre la fraude d'être informées au mieux des avancées réalisées par les « pirates » informatiques et d'élaborer, de façon concertée, des moyens de lutte contre ces attaques.

## II.- ACCROITRE LA PROTECTION DES TITULAIRES DE CARTE

Il a déjà été indiqué que le régime juridique de la carte de paiement est essentiellement de nature contractuelle. Les droits et obligations des trois parties prenantes – établissements de crédit, porteurs de carte et commerçants affiliés – sont effectivement définis par deux types de contrats : le contrat « adhérent » (ou contrat « porteur ») entre l'émetteur de la carte et le titulaire de la carte, d'une part, et le contrat « fournisseur », entre l'émetteur et le commerçant affilié, d'autre part.

S'agissant plus particulièrement du contrat « porteur » de carte bancaire « CB », il convient de noter qu'il s'agit, en général, d'un contrat propre à l'émetteur. Il contient des clauses types élaborées par le GIE et des clauses spécifiques, qui peuvent être liées aux capacités techniques ou à la politique commerciale de l'émetteur.

Le rapport réalisé dans le cadre du Conseil national de la consommation a souligné que les organisations de consommateurs souhaitaient un rééquilibrage des droits entre les deux parties au contrat « porteur » et que certaines d'entre elles avaient demandé l'institution d'un cadre légal.

Votre Rapporteur pour avis considère également que la loi doit se substituer aux règles contractuelles, en ce qui concerne certains aspects de la relation émetteur-porteur. Plusieurs éléments l'incitent à aller dans ce sens.

Tout d'abord, il y est encouragé par les déclarations du ministre de l'économie, des finances et de l'industrie, affirmant qu'« *afin que la*

*puissance publique puisse exercer pleinement son rôle de sécurité, la carte de paiement ne peut pas demeurer un système seulement contractuel* ».

Ensuite, il estime que la liberté contractuelle ne saurait conduire à laisser perdurer des situations inéquitables ou, au sens juridique de ce terme, abusives [(1)]. Or, dans une recommandation adoptée le 17 décembre 1991, la Commission des clauses abusives a formulé de nombreuses remarques, tendant en particulier à l'élimination de certaines clauses des contrats « porteurs », remarques qui – près de dix ans plus tard – n'ont pas encore été intégralement suivies d'effet.

Il est à souligner, d'ailleurs, que cette recommandation de la Commission des clauses abusives n'a pu être publiée au *Journal officiel* que le 27 septembre 1994 (recommandation n° 9402 relative aux contrats porteurs des cartes de paiement assorties ou non d'un crédit), soit près de trois ans après son adoption.

Enfin, il est à noter que la France ne serait pas le premier pays à intervenir par voie législative, dans ce domaine. Ainsi, dès 1978, le Congrès américain a adopté l'« *Electronic fund transfers act* », qui précise le cadre général des droits, devoirs et responsabilités des intervenants dans les systèmes électroniques de paiement. Cette loi protège notamment le consommateur contre des transactions non autorisées ou erronées. Plus récemment et dans un pays de l'Union européenne, le *Folketing* (parlement danois) a adopté la loi n° 414 du 31 mai 2000, fixant le montant maximal de la franchise susceptible d'être mise à la charge du titulaire de la carte.

Dès lors, votre Rapporteur pour avis souhaite proposer à l'Assemblée nationale l'adoption de plusieurs dispositions relatives à la responsabilité du porteur, au délai qui lui est octroyé pour contester un paiement ou un retrait et à son information sur les actualisations du contrat le liant à l'émetteur. Ces diverses mesures pourraient constituer une nouvelle section au sein du chapitre premier du tire II du livre premier du code de la consommation.

### A.- DES RESPONSABILITES CLAIREMENT DEFINIES

Le législateur pourrait fixer le montant maximum de la franchise à la charge du titulaire de la carte, en cas de perte ou de vol. Il pourrait également indiquer expressément qu'en cas d'utilisation frauduleuse de la

---

*(1) Aux termes de l'article L. 132-1 du code de la consommation, «* dans les contrats conclus entre professionnels et non-professionnels ou consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du non-professionnel ou du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat *».*

carte, le titulaire doit être remboursé dans un délai d'un mois et que ce remboursement doit couvrir la totalité des frais supportés.

### 1.- La franchise mise à la charge du porteur en cas de perte ou de vol ne doit pas excéder 150 euros

Dans la charte qu'ils ont signée le 22 février 2001, les établissements de crédit, la Fédération bancaire française et le Groupement des cartes bancaires s'engagent à limiter le montant de la franchise laissée à la charge des porteurs, pour ce qui concerne la fraude antérieure à la déclaration de perte ou de vol, à 400 euros (2.623,83 francs), si le porteur a fait opposition immédiatement (dans les 24 heures) et s'il n'a pas commis une négligence.

Cet engagement constitue un progrès au regard de la situation prévalant antérieurement : pour les paiements, la franchise était de l'ordre de 3.000 francs, tandis que pour les retraits, le porteur supportait généralement la totalité de la perte subie avant la mise en opposition.

Cependant, cet engagement apparaît encore trop restrictif sur deux points. Tout d'abord, le plafond de la franchise devrait être fixé à 150 euros (983,94 francs), comme le préconise également le rapport rédigé dans le cadre du Conseil national de la consommation. Ensuite, la franchise devrait bénéficier au porteur ayant fait opposition avant l'expiration d'un délai de deux jours francs après la perte ou le vol.

- **Un montant conforme à des recommandations européennes**

La recommandation de la Commission européenne 88/590/CEE du 17 novembre 1988 concernant les systèmes de paiement et en particulier les relations entre titulaires et émetteurs de cartes prévoit, au point 83 de l'annexe qui lui est jointe, que le titulaire contractant supporte la perte subie jusqu'au moment de la notification de l'opposition «*jusqu'à un seuil équivalent à 150 écus* ».

Une autre recommandation, plus récente, 97/489/CE du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, dispose au point 1 de son article 6, que «*jusqu'à la notification, le titulaire est responsable des pertes consécutives à la perte ou au vol du moyen de paiement électronique, dans la limite d'un plafond qui ne peut dépasser 150 écus* ».

La position des instances européennes a donc été clairement énoncée et réaffirmée : le montant de la franchise ne doit pas excéder 150 euros [(1)].

Cependant, les émetteurs membres du GIE cartes bancaires ont refusé, jusqu'à présent, de se conformer à ces recommandations, en invoquant plusieurs arguments peu convaincants.

– Ils ont fait valoir, en premier lieu, que les recommandations n'ont aucune valeur contraignante, mais seulement un caractère incitatif.

Cette argumentation, juridiquement exacte, relève néanmoins d'un juridisme étroit. En tout état de cause, elle ne saurait être opposé au législateur, puisque justement si ces actes de la Commission avaient revêtu un caractère obligatoire, il ne serait pas tenu d'intervenir.

En outre, il convient de signaler que la direction générale « marché intérieur » de la Commission européenne a commandé une étude sur l'application de la recommandation de 1997 dans les Etats membres, dont les conclusions seront rendues publiques dans les prochains mois. Il serait donc opportun que la France apparaisse dans cette étude comme un bon élève, d'autant qu'elle est un des Etats où la carte de paiement est le plus employée.

– À cet égard, le deuxième argument invoqué à l'encontre d'une franchise de 150 euros est justement le fait que ce moyen de paiement est d'un usage courant en France, ce qui placerait notre pays dans une situation atypique en Europe (et donc le dispenserait de mettre en œuvre les recommandations précitées).

Cette explication présente un caractère pour le moins paradoxal, car elle conduit à affirmer que plus un moyen de paiement est utilisé, plus son porteur devrait subir les conséquences de la fraude dont il viendrait à être victime, alors même que cette fraude a finalement plus d'occasion d'être réalisée.

– La troisième raison mise en avant par les émetteurs membres du Groupement des cartes bancaires est la nécessaire responsabilisation des porteurs.

Si l'on adopte leur logique, un plafond de 150 euros serait trop faible et conduirait à abaisser la vigilance des porteurs contre le vol ou la perte de leur carte.

---

*(1) Le Règlement du Conseil n° 1103/97 du 17 janvier 1997 prévoit le remplacement, au 1er janvier 1999, de l'écu par l'euro, au taux de 1 euro pour 1 écu.*

Outre le fait qu'une somme de 150 euros est loin d'apparaître négligeable pour la plupart de nos concitoyens, ce raisonnement ignore les désagréments psychologiques et matériels (en particulier, les démarches à accomplir) d'un vol ou d'une perte, qui peuvent suffire à responsabiliser les porteurs d'une carte bancaire.

A titre comparatif, il peut être rappelé que les porteurs, en France, d'une carte *American express* n'encourent, en cas de perte ou de vol, qu'une franchise de 250 francs pour les paiements (en revanche, il sont responsables de la totalité des retraits effectués, sauf en cas d'agression).

Il importe de noter qu'aux Etats-Unis, la « *Regulation E* » qui met en œuvre l'« *Electronic Fund transfers act* », prévoit une responsabilité financière plafonnée à 50 dollars (soit un montant sensiblement inférieur à 150 euros) en cas de notification rapide de la perte ou du vol.

– Le dernier argument développé contre une franchise plafonnée à 150 euros est le risque que les émetteurs cherchent à compenser cette mesure par une hausse des cotisations annuelles acquittées par les porteurs.

Il est quelque peu surprenant que les émetteurs « CB », qui ne manquent jamais une occasion de rappeler que leurs efforts contre la fraude les distinguent de certains concurrents étrangers intégrant la fraude dans le coût des cartes, puissent faire valoir le risque de hausse des cotisations.

Par ailleurs, comme cela a déjà été indiqué au chapitre premier, les émetteurs n'ont pas attendu une éventuelle baisse de la franchise pour augmenter leurs cotisations annuelles : le prix de la carte internationale à débit différé a ainsi subi une hausse de 82% entre 1986 et 2000.

En tout état de cause, les banques françaises qui viennent d'annoncer successivement des bénéfices record en 2000 semblent en mesure de supporter le coût d'une franchise plafonnée à 150 euros.

● **Un délai raisonnable pour effectuer la mise en opposition**

L'engagement souscrit par les banques le 22 février dernier n'accorde le bénéfice de la franchise que si la mise en opposition est effectuée dans les vingt-quatre heures suivant le vol ou la perte de la carte.

Ce délai apparaît exagérément bref, si l'on se rappelle qu'en moyenne, une carte réalise environ 115 opérations par an, soit une tous les trois jours.

On peut d'ailleurs observer qu'aux Etats-Unis, la « *Regulation E* » précitée accorde le bénéfice de la franchise de 50 dollars aux porteurs ayant notifié le vol ou la perte de leur carte dans les quarante-huit heures.

Dès lors, il serait souhaitable d'accorder un délai de deux jours francs pour effectuer la mise en opposition et bénéficier de la franchise.

Bien évidemment, la franchise ne serait pas accordée au porteur ayant agi avec négligence. La recommandation de la Commission européenne du 30 juillet 1997 utilise la notion de « négligence extrême », mais, celle-ci n'existant pas en droit français, il serait plus opportun d'exclure du bénéfice de la franchise, le porteur ayant fait preuve d'une négligence constituant une faute lourde.

De même, il importe de rappeler que cette franchise ne concerne que les pertes subies à la suite d'un vol ou d'une perte. En cas d'usage frauduleux de la carte, le porteur ne doit subir aucun perte, ce qui signifie qu'aucune franchise ne doit lui être opposée et, plus encore, que l'émetteur doit lui rembourser la totalité des frais supportés.

### 2.- La responsabilité du porteur ne doit pas être engagée en cas d'utilisation frauduleuse de sa carte

La recommandation de la Commission européenne du 30 juillet 1997 prévoit également, au point 3 de l'article 6, que « *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). La seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire.* »

Cette rédaction constitue une avancée significative par rapport au texte de la recommandation du 17 novembre 1988 qui proposait l'application d'une franchise en cas de contrefaçon du moyen de paiement.

Elle est également plus favorable aux porteurs que celle retenue par l'article 8 de la directive 97/7/CE sur la vente à distance, actuellement en cours de transposition en droit français. La directive ne prévoit, en effet, le remboursement intégral du porteur victime d'un débit frauduleux que si ce dernier est consécutif au règlement d'un achat à distance réalisé par un tiers, ce qui exclut notamment les fraudes à la « *white plastic* ».

Cependant, il importe de constater que dans la charte signée le 22 février dernier, les banques françaises se sont engagées 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* ». Cette formulation ne vise donc pas que les fraudes réalisées dans le cadre d'un contrat de vente à distance et se rapproche de celle de la recommandation du 30 juillet 1997, que le législateur pourrait reprendre (d'autant que la charte précitée n'engage pas tous les émetteurs).

### 3.- L'émetteur de la carte doit rembourser à son titulaire la totalité des frais supportés en cas d'utilisation frauduleuse

Conformément à une recommandation du rapport réalisé dans le cadre du Conseil national de la consommation, il convient de préciser que l'émetteur doit rembourser les préjudices directs et indirects subis par le porteur d'une carte de paiement ou de retrait ayant fait l'objet d'une utilisation frauduleuse.

Ainsi, le porteur n'aurait à supporter ni le montant des paiements ou retraits frauduleux et, le cas échéant des agios, les frais de mise en opposition, de renouvellement de la carte, etc.

## B.- UN DELAI DE CONTESTATION UNIFORMISE

L'article 13 du contrat porteur « CB » prévoit que le titulaire de la carte a la possibilité de déposer une réclamation dans un délai de 120 jours au maximum, ce qui signifie que certains membres du GIE appliquent un délai inférieur (selon les organisations de consommateurs, certaines banques pratiquent un délai de 30 jours).

Il serait donc nécessaire que la loi fixe, de façon uniforme, le délai de contestation à 120 jours à compter de la date de l'opération contestée.

Des associations de consommateurs souhaiteraient un délai plus étendu, mais les professionnels de la vente à distance estiment qu'un allongement de ce délai fragiliserait davantage les opérateurs du secteur. En outre, on peut raisonnablement penser qu'une période de 120 jours est suffisante pour qu'un porteur puisse s'apercevoir qu'il a été victime d'une ou plusieurs opérations frauduleuses. A titre de comparaison, la « *Régulation E* » précitée n'accorde au consommateur qu'un délai de 60 jours à compter de l'envoi du relevé bancaire.

### C.- UNE MEILLEURE INFORMATION SUR LES MODIFICATIONS DU CONTRAT PORTEUR

Le contrat porteur du GIE cartes bancaires a connu plusieurs versions depuis la création du Groupement. Depuis le 4 septembre 1998, la version 7 est proposée aux nouveaux titulaires d'une carte « CB », mais une version 8 devrait être prochainement adoptée pour prendre en compte les engagements souscrits dans la charte du 22 février 2001.

Cependant, une nouvelle version n'annule pas les versions précédentes, qui continuent à régir les relations entre les émetteurs et les titulaires ayant demandé une carte au moment où ces versions correspondaient à la dernière adoptée par le GIE. Dès lors, de nouvelles garanties contractuelles peuvent ne pas être étendues aux anciens porteurs.

Il conviendrait donc de prévoir que les modifications apportées par l'émetteur aux conditions du contrat doivent être systématiquement portées à la connaissance de tous les titulaires de la carte, par écrit, dans un délai de deux mois maximum. Ces modifications seraient applicables un mois après leur notification si le titulaire du contrat donne son accord, par écrit, dans ce délai. En outre, lors de chaque renouvellement du support (tous les deux ans), l'émetteur devrait proposer au porteur de la carte une actualisation des conditions de son contrat.

*
* *

Au total, votre Rapporteur pour avis approuve les dispositions du projet de loi relatif à la sécurité quotidienne concernant la sécurité des cartes de paiement (articles 7 à 12 et 16), mais il souhaiterait que des correctifs soient apportés aux dispositions de l'article 8 définissant les compétences de la Banque de France en matière de sécurité des moyens de paiement. Il serait souhaitable, par ailleurs, de mettre à profit l'examen du présent projet de loi pour compléter le code de la consommation par des dispositions précisant les droits et obligations des parties au contrat de titulaire d'une carte de paiement ou d'une carte de retrait.

En tout état de cause, votre Rapporteur poursuivra, dans les prochaines semaines, la mission d'information sur les cartes bancaires dont la Commission des finances, de l'économie générale et du Plan l'a chargé. Le présent rapport n'a pas épuisé, en effet, tous les aspects de ce problème, qu'il s'agisse, par exemple, de l'étude des mesures de sécurisation annoncées par les secteurs de la banque et du commerce, de l'examen des

multiples initiatives internationales, des problèmes soulevés par le contrat « fournisseur » conclu par un émetteur et un commerçant affilié, ou encore des perspectives de sécurisation à moyen et à long terme.

## EXAMEN EN COMMISSION

La Commission des finances, de l'économie générale et du Plan a procédé à l'examen pour avis, lors de sa séance du 18 avril 2001, du projet de loi relatif à la sécurité quotidienne.

**Votre Rapporteur pour avis** a noté qu'en matière de sécurité des cartes bancaires, une vive inquiétude avait été ressentie, ces derniers mois, par le grand public et largement médiatisée, notamment à l'occasion de l'affaire « Humpich » et de sa gestion maladroite par le Groupement des cartes bancaires.

Afin de maintenir la confiance dans un instrument de paiement qui a permis de réaliser 26% des paiements en 1999 et de ne pas porter atteinte à l'industrie française de la puce, il était donc essentiel de réagir rapidement. C'est pourquoi il avait proposé, en mai 2000, de travailler sur ce problème, ce qui a conduit la Commission des finances à le charger d'un rapport d'information, dont le rapport pour avis sur le présent projet de loi constitue, en quelque sorte, un rapport d'étape. Il a ajouté que son intention n'était pas de mettre en cause la carte à puce et que, d'ailleurs, toutes les auditions qu'il a réalisées confirment la fiabilité de ce moyen de paiement.

Votre Rapporteur pour avis a rappelé que le Gouvernement, sous l'impulsion de Mme Marylise Lebranchu, alors secrétaire d'Etat aux petites et moyennes entreprises, au commerce et à l'artisanat, s'était également saisie du problème et que diverses mesures de sécurisation ont été prises par MM. Laurent Fabius et François Patriat le 22 février dernier. Ont ainsi été annoncées les mesures législatives figurant dans le présent projet de loi et divers engagements des professionnels concernés, formalisés par la signature de deux chartes. Le ministre de l'économie, des finances et de l'industrie a alors clairement mentionné qu'il s'agissait d'un premier train de mesures ayant vocation à être prolongé.

Votre Rapporteur pour avis a considéré qu'il est possible, dès à présent, de compléter le dispositif législatif proposé, en prévoyant, d'une part, de conforter les compétences de la Banque de France, et, d'autre part, de renforcer la protection des consommateurs.

Il serait ainsi utile de rendre obligatoire la publication au *Journal officiel* des avis négatifs que la Banque de France est susceptible d'émettre. Surtout, la Banque de France doit être dotée d'un véritable pouvoir d'opposition à la mise en service de tout moyen de paiement insuffisamment

sécurisé. Un tel pouvoir aurait probablement évité l'affaire « Humpich », qui n'a pu survenir qu'à la suite de l'inaction du Groupement des cartes bancaires, pourtant informé depuis 1988 d'une faille dans son dispositif. La Banque de France doit également pouvoir disposer de capacités d'expertise et de communication d'informations étendues aux terminaux associés aux moyens de paiement. La création de deux nouveaux organismes – l'Observatoire de la sécurité des cartes bancaires et le Comité de veille technologique pour les systèmes de paiement – apparaît également nécessaire pour assister la Banque de France dans ses nouvelles missions.

Le dispositif gouvernemental peut, par ailleurs, être complété pour accroître la protection des titulaires de carte. C'est ainsi que la franchise supportée par le porteur en cas de perte ou de vol ne doit pas excéder 150 euros, montant conforme à une recommandation de la Commission européenne du 30 juillet 1997. Un délai raisonnable, de deux jours francs, doit aussi être accordé au porteur pour effectuer la mise en opposition. En outre, la responsabilité du porteur ne doit pas être engagée en cas d'utilisation frauduleuse de sa carte et l'émetteur doit lui rembourser aussi bien les préjudices directs que les préjudices indirects. Dans le même esprit, il conviendrait d'uniformiser le délai de contestation à 120 jours à compter de la date de l'opération contestée. Il serait, enfin, judicieux d'assurer l'information systématique des titulaires de carte sur les nouvelles versions du contrat « porteur ».

**M. Jean-Jacques Jégou** a indiqué que, le 22 février dernier, une charte a été signée entre le Gouvernement et le Groupement des cartes bancaires, aux fins d'améliorer les services rendus, notamment dans le domaine de la sécurité. Bien que les cartes à puce apportent déjà une réelle garantie, les professions concernées se sont engagées à effectuer des investissements pour sécuriser le service à hauteur de 7 milliards de francs sur sept ans. S'agissant de la détermination du montant de la franchise et du délai d'opposition, la réduction de la franchise devrait être associée à la réduction du délai pour faire opposition. Or, l'Autorité de régulation des télécommunications s'opposerait à la mise en circulation d'un numéro de téléphone à trois chiffres pour faciliter les opérations de mise en opposition. Enfin, le nouveau rôle confié à la Banque de France paraît contestable, dans la mesure où elle serait juge et partie puisqu'elle est membre du Groupement des cartes bancaires. Sous ces réserves, le texte n'appellerait pas d'opposition particulière.

La Commission est ensuite passée à l'examen des articles 7 à 12 et 16, dont elle est saisie pour avis.

**Article 7 :** *Modification des clauses autorisant l'opposition au paiement par carte :*

La Commission a examiné un amendement de M. Jean-Jacques Jégou, visant à préciser que seuls les cas d'utilisation frauduleuse du numéro de la carte permettent de faire opposition, en dehors des hypothèses du vol et de la perte.

**Votre Rapporteur pour avis** s'est opposé à l'amendement, qui correspond à une interprétation restrictive des cas d'opposition, alors que la rédaction proposée permet une application plus large.

La Commission a *rejeté* cet amendement.

La Commission a émis un *avis favorable à l'adoption* de l'article 7.

**Après l'article 7 :**

La Commission a examiné, en discussion commune, deux amendements présentés respectivement par votre Rapporteur pour avis et Mme Nicole Bricq, visant à introduire un article additionnel qui ramènerait à 150 euros, au lieu de 400 euros, le montant de la franchise laissée à la charge des porteurs pour ce qui concerne la fraude antérieure à la déclaration de perte ou de vol et à prolonger de 24 heures le délai pour faire opposition, en le portant à deux jours francs.

**Votre Rapporteur pour avis** a précisé que le montant de la franchise proposé par son amendement est conforme aux recommandations des autorités communautaires et qu'il est curieux de constater que les banquiers se soumettent à ces recommandations uniquement lorsqu'elles leur conviennent. Il a ajouté que les porteurs de cartes *American Express* n'encourent qu'une franchise de 250 francs en cas de perte ou de vol, pour les paiements effectués.

**Mme Nicole Bricq** a observé que les deux amendements reflètent une revendication unanime des associations de défense des consommateurs, notamment en ce qui concerne la prolongation du délai d'opposition. Il serait, cependant, préférable de ne pas retenir la notion de « négligence extrême » mentionnée dans l'amendement de votre Rapporteur pour avis, son contenu juridique étant plus qu'incertain.

**M. Jean-Jacques Jégou** a estimé que l'octroi du bénéfice de la franchise aux porteurs faisant opposition dans le délai de deux jours accroîtrait le risque de manœuvres frauduleuses. La réduction à 150 euros de la franchise serait acceptable, à la condition que le propriétaire de la carte

puisse prouver qu'il a tout mis en œuvre pour faire opposition dans les délais les plus brefs.

**Votre Rapporteur pour avis** a rappelé que le texte en discussion concerne l'utilisation de la carte en cas de vol ou de perte et non une autre forme d'utilisation frauduleuse. De surcroît, le numéro de téléphone unique pour faire opposition existe déjà et figure sur tous les distributeurs de billets. S'agissant des chartes du 22 février dernier, elles ont été signées par les représentants des professions bancaires, d'une part, et par le Conseil du commerce de France, d'autre part, et non entre le Gouvernement et le Groupement des cartes bancaires. Ce dernier s'est engagé à mettre réellement en œuvre des engagements précédents non tenus, par exemple en matière de sécurisation de tous les distributeurs automatiques de billets, qui devraient tous être prochainement équipés pour lire la puce.

Votre Rapporteur pour avis a également précisé qu'une « négligence extrême » constituait une faute lourde et que cette notion figurait dans la recommandation de la Commission européenne du 30 juillet 1997. La France souhaite, en effet, une extension des cartes à puces dans le cadre du marché communautaire, en s'inspirant des règles communautaires. Il a ajouté que le texte du projet de loi visait à assurer, lorsqu'un dysfonctionnement d'un moyen de paiement est détecté, une publication de cette information, ainsi que celle de la mise en conformité du niveau de sécurité lorsque celle-ci est rétablie. Cette mesure est donc de nature à assurer notamment une transparence du Groupement des cartes bancaires.

Votre rapporteur pour avis a aussi souligné que la mise en opposition dans les quarante-huit heures lui paraissait de nature à limiter sensiblement un usage frauduleux des cartes à puce.

Rappelant que le montant annuel de cette fraude s'élevait en France à 250 millions de francs pour les paiements, **M. Jean-Jacques Jégou** a souhaité savoir à combien elle se montait aux Etats-Unis.

**M. Pierre Hériaud** a précisé que la fraude aux Etats-Unis était environ dix fois plus élevée qu'en France, où elle avait particulièrement diminué ces dix dernières années.

**Votre Rapporteur pour avis** a précisé, à cet égard, que d'après le Groupement des cartes bancaires, la fraude ne soulevait de véritable problème économique aux établissements bancaires qu'au-delà d'un taux de 0,03% – 0,04%. Le taux de fraude quantifiée par le Groupement ne prend d'ailleurs en compte que la fraude mise à la charge des établissements bancaires, et non pas celle à la charge des porteurs de cartes ou des commerçants. De manière plus générale, il a souligné que les dispositions

du projet de loi visaient à responsabiliser l'ensemble des parties intéressées au fonctionnement des cartes à puce, qu'il s'agisse des particuliers, des commerçants ou des établissements bancaires, et d'anticiper les risques de fraude liés à l'évolution technologique. Il est vrai, enfin, que, sur les sept prochaines années, sept milliards de francs d'investissements seront nécessaires pour sécuriser les cartes bancaires, mais l'essentiel de ces sommes sera à la charge des commerçants, et non à celle des établissements bancaires.

Après que **Mme Nicole Bricq** eut souligné l'absence de définition juridique précise de la notion de « négligence extrême », **votre Rapporteur pour avis** a indiqué que celle-ci ne manquait pas de pertinence : en retenant une notion figurant d'ores et déjà dans le droit communautaire, le législateur incitera ainsi le juge à l'interpréter de manière constructive.

**Le Président Henri Emmanuelli** a fait valoir qu'en l'absence de définition de la notion de « négligence extrême », le législateur laisserait à la jurisprudence le soin de préciser le dispositif envisagé.

**M. Jean-Jacques Jégou** a souligné les risques du dispositif retenu : la fixation du montant de la franchise à 150 euros, au lieu de 400 euros actuellement, en cas de perte ou de vol, et l'octroi de deux jours francs au titulaire, au lieu de 24 heures actuellement, pour effectuer la mise en opposition constituent un risque supplémentaire de fraude, dont on ne sait qui, des commerçants ou du Groupement des cartes bancaires, en supportera le coût.

**Votre Rapporteur pour avis** a contesté cette appréciation, faisant valoir que les porteurs d'une carte « *American express* » n'encourent qu'une franchise de 250 francs pour les paiements, mesure qui ne semble pas avoir été source de phénomènes massifs de fraude.

**Le Président Henri Emmanuelli** a rappelé, à cet égard, que l'importance de la fraude à la carte bancaire avait sensiblement diminué en France au cours des dix dernières années, passant d'un rapport de dix à un.

**Votre Rapporteur pour avis** a souligné que les dispositions prévues au titre du présent projet de loi permettraient de renforcer sensiblement les mesures visant à prévenir ces risques de fraude. Il a, néanmoins, proposé de rectifier son amendement afin de préciser que le titulaire d'une carte ne bénéficie d'aucune franchise s'il a agi avec une négligence « constituant une faute lourde ».

La Commission a *adopté* l'amendement de votre Rapporteur pour avis (**amendement n° 4**) et a *rejeté* l'amendement de Mme Nicole Bricq.

La Commission a ensuite examiné, en discussion commune, deux amendements présentés par votre Rapporteur pour avis et Mme Nicole Bricq, tendant respectivement, pour le premier, à affirmer, conformément aux termes de la recommandation de la Commission européenne du 30 juillet 1997, l'absence de responsabilité du titulaire de la carte en cas d'utilisation frauduleuse de sa carte, et pour le second, à définir les modalités de recréditation du compte bancaire d'une personne victime d'une utilisation frauduleuse de sa carte dans le cadre d'un contrat de vente à distance.

Après que **votre Rapporteur pour avis** eut précisé que ce second dispositif était d'une portée plus limitée, la Commission a *adopté* l'amendement présenté par votre Rapporteur pour avis (**amendement n° 5**) et a *rejeté* l'amendement de Mme Nicole Bricq.

La Commission a examiné un amendement de votre Rapporteur pour avis, proposant de rembourser les préjudices directs et indirects subis par le porteur d'une carte de paiement ou de retrait ayant fait l'objet d'une utilisation frauduleuse.

**Votre Rapporteur pour avis** a précisé qu'ainsi les titulaires n'auraient à supporter ni le montant des paiements ou des retraits frauduleux et, le cas échéant, des agios, ni les frais de mise en opposition et de renouvellement de la carte.

La Commission a *adopté* cet amendement (**amendement n° 6**).

Elle a ensuite *adopté* un amendement de votre Rapporteur pour avis, tendant à uniformiser le délai de contestation accordé au porteur, en le fixant à 120 jours (**amendement n° 7**).

La Commission a examiné un amendement de votre Rapporteur pour avis, visant à permettre au titulaire de la carte de bénéficier de la version la plus récente du contrat, puisque ce dernier est régulièrement modifié.

**Votre Rapporteur pour avis** a rappelé que le contrat porteur « CB » en était à sa septième version et devrait prochainement faire l'objet d'une huitième version. Il a précisé que, dans un souci de responsabilisation du porteur, les modifications apportées par l'émetteur aux conditions du contrat seraient portées à la connaissance du titulaire de la carte, ce dernier disposant d'un délai d'un mois pour manifester son accord.

La Commission a *adopté* cet amendement (**amendement n° 8**).

Elle a ensuite *adopté* un amendement rédactionnel de votre Rapporteur pour avis, insérant un titre de section après l'article L. 12482 du code de la consommation (**amendement n° 9**).

**Article 8 :** *Renforcement des pouvoirs de la Banque de France en matière de sécurité des moyens de paiement :*

La Commission a examiné un amendement présenté par M. Jean-Jacques Jégou, tendant à supprimer les dispositions prévoyant que la Banque de France s'assure de la pertinence des normes applicables en matière de sécurité des paiements.

**M. Jean-Jacques Jégou** a estimé, tout d'abord, que la Banque de France n'était pas habilitée à intervenir à l'encontre des émetteurs étrangers puisque la loi de 1993, portant statut de la Banque de France, ne comprenait pas cette mission, et, ensuite, qu'en tant que membre du Groupement des cartes bancaires, elle serait, en quelque sorte, juge et partie.

**Votre Rapporteur pour avis** a observé que la Banque de France était seulement observateur au sein du Groupement des cartes bancaires.

La Commission a *rejeté* cet amendement.

Elle a ensuite examiné un amendement de M. Jean-Jacques Jégou, visant à supprimer les dispositions aux termes desquelles la Banque de France disposerait de la possibilité de formuler un avis négatif à l'encontre de la sécurité d'un moyen de paiement et de rendre cet avis public.

**M. Jean-Jacques Jégou** a souligné que les émetteurs de moyens de paiement n'auraient aucun recours pour contester cet avis.

**Votre Rapporteur pour avis** a souligné que l'avis publié n'aurait pas de valeur juridique, mais aurait certainement un fort impact moral.

**Le Président Henri Emmanuelli** a rappelé que la Banque de France avait pour mission de dresser la liste des interdits bancaires et qu'en conséquence il n'y avait pas d'objection déontologique à ce qu'elle puisse se prononcer sur la sécurité des moyens de paiement.

**Votre Rapporteur pour avis** a souhaité que le système français soit progressivement étendu à l'Union européenne et a estimé qu'une telle procédure valoriserait et validerait notre technologie. Il a rappelé, en outre, qu'il proposait deux mesures importantes en la matière, à savoir la création de l'Observatoire de la sécurité des cartes bancaires et d'un Comité de veille technologique pour les systèmes de paiement.

La Commission a *rejeté* cet amendement.

La Commission a *adopté* un amendement présenté par votre Rapporteur pour avis, visant à rendre obligatoire la publication des avis négatifs par une insertion au *Journal officiel* (**amendement n° 10**).

Elle a ensuite *adopté* un amendement présenté par votre Rapporteur pour avis, autorisant la Banque de France à s'opposer à la mise à disposition du public de toute carte de paiement dont les fonctions de sécurité seraient insuffisantes (**amendement n° 11**), un amendement de Mme Nicole Bricq, tendant au même objet étant considéré comme satisfait.

La Commission a *adopté* un amendement de votre Rapporteur pour avis, étendant aux terminaux ou aux dispositifs techniques associés aux moyens de paiement, les compétences de la Banque de France en matière d'expertise et de communication d'informations (**amendement n° 12**).

La Commission a ensuite examiné deux amendements, visant à créer un Observatoire de la sécurité des cartes bancaires :

– l'un, présenté par votre Rapporteur pour avis, visant à confier à la Banque de France la présidence de l'observatoire, le secrétariat de ce dernier étant confié à un représentant des associations de consommateurs ;

– l'autre, présenté par Mme Nicole Bricq, tendant à confier à la Banque de France le secrétariat général de cet observatoire, sa présidence étant assurée par une personne qualifiée choisie parmi les membres de l'observatoire.

**Mme Nicole Bricq** a indiqué que son amendement laissait davantage ouvert le choix du président, même s'il n'était pas certain que les associations de consommateurs désireraient assurer cette fonction.

**Votre Rapporteur pour avis** a déclaré préférer sa rédaction, même si la discussion pourrait utilement se prolonger en séance publique.

La Commission a *rejeté* l'amendement de Mme Nicole Bricq et a *adopté* l'amendement de votre Rapporteur pour avis (**amendement n° 13**).

La Commission a examiné un amendement de votre Rapporteur pour avis, proposant d'instituer un Comité de veille technologique pour les systèmes de paiement, dont le secrétariat serait assuré par la Banque de France, et qui serait composé de représentants des administrations concernées et chargé de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des systèmes de paiement.

**Votre Rapporteur pour avis** a considéré qu'il s'agissait de permettre aux administrations chargées de la lutte contre la fraude d'être informées au mieux des avancées réalisées par les pirates informatiques et d'élaborer en concertation des moyens de lutte contre ces attaques.

**Mme Nicole Bricq** s'est interrogée sur l'opportunité de confier à la Banque de France, dans le cadre d'un nouvel organisme, un rôle qu'elle exerce déjà au sein d'un organisme similaire existant, rattaché au Secrétariat général de la Défense nationale. Les données concernant la sécurité des systèmes de paiement sont, par ailleurs, extrêmement confidentielles et doivent faire l'objet de la diffusion la plus restreinte possible.

**Votre Rapporteur pour avis** a indiqué que le rôle de la Banque de France dans le comité dépendant du ministère de la Défense était extrêmement informel et que, par ailleurs, la composition du Comité de veille technologique serait extrêmement restreinte en étant limitée aux représentants des ministères concernés, notamment la Justice, les Finances et l'Intérieur.

**M. Jean-Jacques Jégou** a considéré que des questions de ce type ne pouvaient pas être utilement abordées dans ce genre de « happening » de fonctionnaires.

**Le Président Henri Emmanuelli** a rappelé que le comité dépendant du Secrétariat général de la Défense nationale s'occupait seulement de cryptologie, et non de la sécurité des systèmes de paiement.

**Votre Rapporteur pour avis** a jugé important que la Banque de France soit associée à ce Comité de veille technologique et qu'il convenait d'associer aussi étroitement que possible les différentes administrations, dans la mesure où l'insuffisance de coopération favorisait toujours les fraudeurs.

**M. Jean-Jacques Jégou** a estimé que le Groupement des cartes bancaires constituerait sans doute le meilleur cadre pour la discussion de ce type de problème.

**Votre Rapporteur pour avis** a précisé que ce Groupement pourrait bien évidemment communiquer éventuellement les informations en sa possession. Par ailleurs, la Banque de France assurerait le secrétariat de ce comité, mais n'en assurerait pas la direction.

**Le Président Henri Emmanuelli** a jugé souhaitable que la direction effective de ce comité soit confiée à l'administration chargée de la

répression des infractions en matière de moyens de paiement, à savoir le ministère de l'intérieur.

**Votre Rapporteur pour avis** a souligné le parallèle entre le dispositif proposé par son amendement et les principes appliqués en matière de lutte contre la fausse monnaie, où la Banque de France assume un rôle éminent sans pour autant être investie du pouvoir de réprimer les infractions y afférentes, qui reste une prérogative étatique.

La Commission a *adopté* cet amendement (**amendement n° 14**), puis a émis un *avis favorable à l'adoption* de l'article 8.

**Article 9 :** *Renforcement de la répression de la falsification ou de la contrefaçon des instruments de la monnaie scripturale :*

La Commission a *rejeté* un amendement présenté par **M. Jean-Jacques Jégou**, tendant à élargir la définition des actes préparatoires à la contrefaçon ou la falsification des moyens de paiement autres que les espèces, **votre Rapporteur pour avis** ayant fait valoir que cet élargissement conduirait à incriminer, le cas échéant, les fournisseurs d'accès à Internet et les gestionnaires de « portails » Internet dont les services auraient été utilisés pour accéder à des sites fournissant des données conçues ou spécialement adaptées pour commettre des fraudes.

La Commission a ensuite émis un *avis favorable à l'adoption* de l'article 9.

**Article 10 :** *Confiscation et destruction des moyens permettant la contrefaçon ou la falsification de la monnaie scripturale :*

La Commission a émis un *avis favorable à l'adoption* de l'article 10.

**Article 11 :** *Peines complémentaires :*

La Commission a émis un *avis favorable à l'adoption* de l'article 11.

**Article 12 :** *Instauration de la responsabilité pénale des personnes morales pour les infractions relatives aux chèques et aux cartes de paiement :*

La Commission a émis un *avis favorable à l'adoption* de l'article 12.

**Article 16 :** *Application à l'outre-mer des dispositions des chapitres II et III du projet de loi :*

La Commission a *adopté* trois amendements de coordination (**amendements n° 15, 16 et 17**), puis émis un *avis favorable à l'adoption* de l'article 16.

# AMENDEMENTS ADOPTES PAR LA COMMISSION

## *Après l'article 7*

**Amendement n° 4 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un article L. 121-83 ainsi rédigé :

« *Art. L. 121-83*. – Le titulaire d'une carte mentionnée à l'article L. 132-1 du code monétaire et financier supporte la perte subie, en cas de perte ou de vol, avant la mise en opposition prévue par l'article L. 132-2 dudit code, dans la limite d'un plafond qui ne peut dépasser 150 euros, sauf s'il a agi avec une négligence constituant une faute lourde ou si la mise en opposition a été effectuée plus de deux jours francs après la perte ou le vol, auxquels cas le plafond prévu n'est pas applicable. »

**Amendement n° 5 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un article L. 121-84 ainsi rédigé :

« *Art. L. 121-84*. – La responsabilité du titulaire d'une carte mentionnée à l'article L. 132-1 du code monétaire et financier n'est pas engagée si la carte a été utilisée sans présentation physique ou sans identification électronique. La seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire. En conséquence, si le titulaire de la carte conteste par écrit avoir effectué un paiement ou un retrait, les sommes contestées lui sont recréditées sur son compte par l'émetteur de la carte ou restituées, sans frais, au plus tard dans le délai d'un mois à compter de la réception de la contestation. »

**Amendement n° 6 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un article L. 121-85 ainsi rédigé :

« *Art. L. 121-85*. – En cas d'utilisation frauduleuse d'une carte mentionnée à l'article L. 132-1 du code monétaire et financier, l'émetteur de la carte rembourse à son titulaire la totalité des frais qu'il a supportés. »

**Amendement n° 7 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un article L. 121-86 ainsi rédigé :

« *Art. L. 121-86.* – Le titulaire d'une carte de paiement ou de retrait a la possibilité de déposer une réclamation dans un délai de 120 jours à compter de la date de l'opération contestée. »

**Amendement n° 8 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un article L. 121-87 ainsi rédigé :

« *Art. L. 121-87.* – Les modifications apportées par l'émetteur aux conditions du contrat sont portées à la connaissance du titulaire de la carte, par écrit, dans un délai de deux mois maximum. Ces modifications sont applicables un mois après leur notification si le titulaire du contrat donne son accord par écrit dans ce délai.

« Lors de chaque renouvellement du support, l'émetteur propose au titulaire de la carte une actualisation des conditions de son contrat. »

**Amendement n° 9 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Insérer l'article suivant :

Après l'article L. 121-82 du code de la consommation, il est inséré un intitulé ainsi rédigé :

« Section 11.- Contrat de titulaire d'une carte de paiement ou d'une carte de retrait. »

## *Article 8*

**Amendement n° 10 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

A la fin de la dernière phrase du deuxième alinéa de cet article, substituer aux mots : « et de le rendre public », les mots : « publié au *Journal officiel* ».

**Amendement n° 11 présenté par M. Jean-Pierre Brard, Rapporteur pour avis, et M^me^ Nicole Bricq :**

Compléter le deuxième alinéa de cet article par la phrase suivante :

« Tout moyen de paiement ayant fait l'objet d'un avis négatif ne peut être émis et circuler tant que son émetteur ne s'est pas conformé aux recommandations de la Banque de France et que celle-ci n'a pas formulé un avis positif publié au *Journal officiel.* »

**Amendement n° 12 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Compléter le dernier alinéa de cet article par les mots :

« , concernant les moyens de paiement et les terminaux ou les dispositifs techniques qui leur sont associés. »

**Amendement n° 13 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Compléter cet article par l'alinéa suivant :

« La Banque de France assure la présidence de l'Observatoire de la sécurité des cartes bancaires, qui regroupe des représentants des administrations concernées, des émetteurs de cartes de paiement, des associations de commerçants et de consommateurs. Le secrétariat de cet observatoire est confié à un représentant des associations de consommateurs. L'Observatoire de la sécurité des cartes bancaires assure, en particulier, le suivi et l'évaluation des mesures de sécurisation entreprises par les émetteurs et les commerçants, ainsi que l'établissement de statistiques de la fraude. Un décret en Conseil d'Etat précise sa composition et ses compétences. »

**Amendement n° 14 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Compléter cet article par l'alinéa suivant :

« La Banque de France assure le secrétariat du Comité de veille technologique pour les systèmes de paiement, composé de représentants des administrations concernées et chargé de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des systèmes de paiement. Un décret en Conseil d'Etat précise sa composition et ses compétences. »

## *Article 16*

**Amendement n° 15 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

A la fin de la dernière phrase du deuxième alinéa du II de cet article, substituer aux mots : « et de le rendre public », les mots : « publié au *Journal officiel* ».

**Amendement n° 16 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Compléter le deuxième alinéa du II de cet article par la phrase suivante :

« Tout moyen de paiement ayant fait l'objet d'un avis négatif ne peut être émis et circuler tant que son émetteur ne s'est pas conformé aux recommandations de l'Institut d'émission d'outre-mer et que celui-ci n'a pas formulé un avis positif publié au *Journal officiel*. »

**Amendement n° 17 présenté par M. Jean-Pierre Brard, Rapporteur pour avis :**

Compléter le dernier alinéa de cet article par les mots :

« , concernant les moyens de paiement et les terminaux ou les dispositifs techniques qui leur sont associés. »

2992 - Avis de M. Jean-Pierre Brard au nom de la commission des finances sur le projet de loi relatif à la sécurité quotidienne.