N° 3229

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

ONZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 juillet 2001.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DES FINANCES, DE L'ÉCONOMIE GÉNÉRALE ET DU PLAN (1),

sur **la sécurité des cartes bancaires**,

ET PRÉSENTÉ

PAR M. Jean-Pierre BRARD,

Député.

___

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

Banques et établissements financiers.

La *Commission des finances, de l'économie générale et du Plan* est composée de : <A HREF="1252.asp"> M. Henri Emmanuelli</A> , *président* ; <A HREF="633.asp"> M. Michel Bouvard</A> , <A HREF="654.asp"> M. Jean-Pierre Brard</A> , <A HREF="2794.asp"> M. Yves Tavernier</A> , *vice-présidents* ; <A HREF="621.asp"> M. Pierre Bourguignon</A> , <A HREF="1723.asp"> M. Jean-Jacques Jégou</A> , <A HREF="2772.asp"> M. Michel Suchod</A> , *secrétaires* ; <A HREF="2189.asp"> M. Didier Migaud</A> , *Rapporteur Général* ; <A HREF="234.asp"> M. Maurice Adevah-Poeuf</A> , <A HREF="294.asp"> M. André Aschieri</A> , <A HREF="301.asp"> M. Philippe Auberger</A> , <A HREF="304.asp"> M. François d'Aubert</A> , <A HREF="339.asp"> M. Dominique Baert</A> , <A HREF="350.asp"> M. Jean-Pierre Balligand</A> , <A HREF="356.asp"> M. Gérard Bapt</A> , <A HREF="369.asp"> M. François Baroin</A> , <A HREF="374.asp"> M. Alain Barrau</A> , <A HREF="378.asp"> M. Jacques Barrot</A> , <A HREF="464.asp"> M. Christian Bergelin</A> , <A HREF="495.asp"> M. Éric Besson</A> , <A HREF="551.asp"> M. Alain Bocquet</A> , <A HREF="581.asp"> M. Augustin Bonrepaux</A> , <A HREF="599.asp"> M. Jean-Michel Boucheron</A> , <A HREF="671.asp"> Mme Nicole Bricq</A> , <A HREF="698.asp"> M. Christian Cabal</A> , <A HREF="706.asp"> M. Jérôme Cahuzac</A> , <A HREF="733.asp"> M. Thierry Carcenac</A> , <A HREF="746.asp"> M. Gilles Carrez</A> , <A HREF="794.asp"> M. Henry Chabert</A> , <A HREF="868.asp"> M. Didier Chouat</A> , <A HREF="872.asp"> M. Alain Claeys</A> , <A HREF="942.asp"> M. Charles de Courson</A> , <A HREF="970.asp"> M. Christian Cuvilliez</A> , <A HREF="1033.asp"> M. Arthur Dehaine</A> , <A HREF="1039.asp"> M. Jean-Pierre Delalande</A> , <A HREF="1079.asp"> M. Yves Deniaud</A> , <A HREF="1116.asp"> M. Michel Destot</A> , <A HREF="1124.asp"> M. Patrick Devedjian</A> , <A HREF="1148.asp"> M. Laurent Dominati</A> , <A HREF="1165.asp"> M. Julien Dray</A> , <A HREF="1166.asp"> M. Tony Dreyfus</A> , <A HREF="1199.asp"> M. Jean-Louis Dumont</A> , <A HREF="1305.asp"> M. Daniel Feurtet</A> , <A HREF="1326.asp"> M. Pierre Forgues</A> , <A HREF="1381.asp"> M. Gérard Fuchs</A> , <A HREF="1407.asp"> M. Gilbert Gantier</A> , <A HREF="1437.asp"> M. Jean de Gaulle</A> , <A HREF="1445.asp"> M. Hervé Gaymard</A> , <A HREF="1588.asp"> M. Jacques Guyard</A> , <A HREF="1631.asp"> M. Pierre Hériaud</A> , <A HREF="1642.asp"> M. Edmond Hervé</A> , <A HREF="1686.asp"> M. Jean-Louis Idiart</A> , <A HREF="1687.asp"> Mme Anne-Marie Idrac</A> , <A HREF="1690.asp"> M. Michel Inchauspé</A> , <A HREF="1774.asp"> M. Jean-Pierre Kucheida</A> , <A HREF="1790.asp"> M. Marc Laffineur</A> , <A HREF="1880.asp"> M. Jean-Marie Le Guen</A> , <A HREF="1980.asp"> M. Maurice Ligot</A> , <A HREF="1994.asp"> M. François Loos</A> , <A HREF="2025.asp"> M. Alain Madelin</A> , <A HREF="2088.asp"> Mme Béatrice Marre</A> , <A HREF="2148.asp"> M. Pierre Méhaignerie</A> , <A HREF="2175.asp"> M. Louis Mexandeau</A> , <A HREF="2207.asp"> M. Gilbert Mitterrand</A> , <A HREF="2560.asp"> M. Jean Rigal</A> , <A HREF="2588.asp"> M. Gilles de Robien</A> , <A HREF="2600.asp"> M. Alain Rodet</A> , <A HREF="2622.asp"> M. José Rossi</A> , <A HREF="2680.asp"> M. Nicolas Sarkozy</A> , <A HREF="2686.asp"> M. Gérard Saumade</A> , <A HREF="2718.asp"> M. Philippe Séguin</A> , <A HREF="2843.asp"> M. Georges Tron</A> , <A HREF="2915.asp"> M. Jean Vila</A> .

Sommaire

Pages

introduction 5

chapitre premier : des relations apaisées entre les émetteurs de cartes et les commerÇants 11

I.- le règlement par la voie contentieuse du conflit relatif à la commission interbancaire de paiement ***12***

A.- le groupement des cartes bancaires sanctionné par le conseil de la concurrence ***12***

b.- l'échec de la fronde des grandes enseignes ***15***

II.- le protocole d'accord du 17 janvier 2001 ***16***

a.- une réponse à la demande de concertation des commerçants ***16***

B.- une mise en œuvre concertée des investissements à entreprendre ***17***

chapitre II : LE PORTE-MONNAIE ÉLECTRONIQUE : DES EXPÉRIENCES MULTIPLES N'AYANT PAS encore DÉPASSÉ LE STADE EXPÉRIMENTAL 19

I.- Un instrument adapté aux paiements de petits montants ***19***

II.- de multiples initiatives en europe ***20***

III.- une expérimentation tardive en France ***22***

CHAPITRE III : LE BESOIN DE SÉCURISATION DU COMMERCE ÉLECTRONIQUE 25

I.- le commerce Électronique ne doit pas être confondu avec le paiement en ligne sur internet ***25***

A.- internet n'est pas le seul vecteur du commerce Électronique ***25***

B.- Le paiement en ligne ne caractérise pas le commerce électronique ***26***

II.- Une forme de commerce encore marginale ***28***

A.- Un développement inférieur aux prévisions ***28***

B.- un problème certain de besoin de sécurité ***29***

III.- des moyens de sécurisation foisonnants ne mettant pas obligatoirement en œuvre la carte à puce ***32***

A.- le virement par banque à distance ***32***

B.- Les systèmes privés de compensation ***33***

c.- Le numéro de transaction unique ***34***

IV.- la sécurisation des transactions réalisées par carte de paiement ***35***

A.- des dispositifs dont le niveau de sécurisation est variable ***35***

B.- les difficultés de la solution* cyber-Comm** ***36

Chapitre IV : Le renforcement nécessaire de l'intervention des pouvoirs publics 39

I.- Achever rapidement la mise en place d'un cadre juridique adapté ***40***

a.- adopter au plus vite les projets de loi relatifs À la sÉcuritÉ quotidienne et sur la sociÉtÉ de l'information ***40***

b.- prendre de nouvelles initiatives ***41***

1.- Impliquer les commerçants dans la sécurisation ***41***

2.- Etudier la mise en place d'une carte de citoyen électronique ***42***

ii.- promouvoir un « modÈle europÉen » ***43***

A.- Favoriser l'apparition de dispositifs interopÉrables et sÉcurisÉs ***43***

B.- préserver l'acquis européen ***45***

examen en commission 47

ANNEXES 51

ANNEXE I : PRINCIPALES PROPOSITIONS CONTENUES DANS LE PRÉSENT RAPPORT D'INFORMATION 53

ANNEXE II : sigles utilisÉs 55

ANNEXE III : liste des personnes entendues 57

introduction

Le présent rapport d'information constitue l'aboutissement d'une démarche entreprise en mai 2000, peu de temps après que l'importante médiatisation de l'« affaire Humpich » eut instillé le doute sur la sécurité du système français des cartes bancaires.

Les différentes étapes de cette démarche ont déjà été décrites dans l'introduction du rapport pour avis sur le projet de loi relatif à la sécurité quotidienne (n° 2992) que votre Rapporteur a rédigé au nom de la Commission des finances, de l'économie générale et du Plan et auquel il se permet de renvoyer.

Ce dernier rapport a été conçu, en effet, comme le rapport d'étape de la mission d'information dont j'ai été chargé. Il a permis, en particulier, d'étudier la réalité de la fraude en France et de formuler diverses propositions, afin de renforcer la confiance des consommateurs dans cet instrument de paiement.

Ces propositions ont, pour l'essentiel, été traduites par des amendements permettant de compléter le dispositif de sécurisation proposé par le Gouvernement dans le projet de loi relatif à la sécurité quotidienne.

Il n'y a pas lieu de se livrer ici à un nouvel examen détaillé dudit projet de loi, qui est encore en discussion et dont l'adoption définitive ne pourra intervenir qu'à l'automne prochain. On se bornera à en rappeler les lignes essentielles, à savoir :

– le renforcement du rôle de la Banque de France en ce qui concerne la sécurité des moyens de paiement scripturaux ;

– l'adaptation du dispositif pénal aux nouvelles formes de criminalité ;

– l'accroissement de la protection des titulaires de carte.

Votre Rapporteur souhaiterait, néanmoins, insister sur deux points, qui lui paraissent constituer des avancées fondamentales.

Tout d'abord, le projet de loi précité prévoit la création d'un Observatoire de la sécurité des cartes de paiement.

Cette instance, dont le secrétariat sera assuré par la Banque de France, devrait favoriser le dialogue et la transparence pour, finalement, conforter la sécurité des cartes de paiement.

L'Observatoire regroupera, en effet, des représentants de toutes les parties

concernées (émetteurs de cartes de paiement, commerçants, consommateurs, administrations et parlementaires), symbolisant l'établissement de rapports équilibrés et la mise en responsabilité de chacun des partenaires, d'autant que, si la présidence devrait revenir à un parlementaire, il est probable que deux co-rapporteurs seront choisis parmi les représentants des commerçants et des consommateurs. Cette composition le distingue nettement du conseil de direction du Groupement des cartes bancaires (qui réunit les onze principaux organismes financiers français) ou de l'Observatoire des systèmes de paiement électronique (), mis en place par les autorités européennes pour favoriser les échanges d'informations entre professionnels du secteur.

Cette composition étendue n'empêchera pas le fonctionnement, en son sein, d'une cellule de veille technologique, associant les administrations chargées de la lutte contre la fraude et permettant une meilleure prévention des nouvelles formes de criminalité, ainsi qu'une coordination plus efficace des actions de lutte engagées.

Le second aspect du projet de loi relatif à la sécurité quotidienne méritant d'être spécialement signalé concerne la définition des droits et obligations des titulaires de carte.

Les dispositions, adoptées à l'initiative de votre Rapporteur, devraient permettre une meilleure protection des consommateurs, ce qui répond aux recommandations formulées par la Commission européenne et ce qui, au final, conforte la confiance dans cet instrument de paiement.

Une meilleure protection des consommateurs :

Les articles 7 *ter* et 7 *quater* du projet de loi précité, qui a fait l'objet d'une nouvelle lecture à l'Assemblée nationale les 26 et 27 juin dernier, permettent de définir précisément la responsabilité des porteurs de carte.

Tandis que l'article 7 *ter* limite la responsabilité de ces derniers en cas de perte ou de vol de leur carte, l'article 7 *quater* pose le principe de l'absence de responsabilité dans les cas d'utilisation frauduleuse de la carte.

Ainsi, en cas de perte ou de vol, le titulaire de la carte ne pourra pas supporter une franchise supérieure à 275 euros (puis à 150 euros à compter du 1er janvier 2003) pour les pertes subies avant la mise en opposition. De plus, la victime d'une utilisation frauduleuse d'une carte qu'elle a pourtant en sa possession ne subira aucune perte financière.

Sur ce dernier point, la disposition adoptée par l'Assemblée nationale en première lecture reprenait, quasiment mot à mot, les termes de la recommandation de la Commission européenne 97/489/EC du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire.

Cette rédaction a néanmoins suscité de vives réactions de la part du Groupement des cartes bancaires, qui a dénoncé des amendements « *inappropriés,*

voire graves » (). Ces inquiétudes, quelque peu exagérées, ont également été partagées, dans des termes plus mesurés, par les représentants des commerçants et par les services de la Commission européenne, qui craignaient une remise en cause du principe de l'irrévocabilité des paiements, dans la mesure où le texte affirmait que « *la seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire* ».

Le Sénat a partagé les mêmes préoccupations que l'Assemblée nationale et il lui a paru légitime que le porteur de carte n'ait pas à supporter les conséquences financières de la fraude. Cependant, pour répondre aux inquiétudes qui se sont manifestées après le vote de l'Assemblée nationale, le Sénat a souhaité préciser clairement, dans le texte de l'article 7 *quater*, que le porteur ne serait déchargé de sa responsabilité qu'en cas d'utilisation «*frauduleuse* » d'un code confidentiel.

Cette version adoptée par le Sénat n'a pas supprimé toutes les réticences. Votre Rapporteur a donc proposé une nouvelle rédaction de l'article 7 *quater*, élaborée en concertation avec les parties intéressées, qui a été adoptée, par l'Assemblée nationale, en nouvelle lecture.

Le nouveau dispositif proposé par l'amendement que j'ai déposé se caractérise, tout d'abord, par une distinction du cas de la vente à distance et de celui de la carte contrefaite (la fameuse « *white plastic* ») utilisée dans le cadre d'un retrait ou d'un paiement en face-à-face. On évite ainsi de remettre en cause les paiements à distance effectués avec des lecteurs sécurisés (tel que *Cyber-comm*).

La nouvelle rédaction de l'article 7 *quater* supprime, ensuite, les formules ambiguës faisant référence au code confidentiel ou à la négligence fautive du porteur. Il sera ainsi permis d'éviter les débats sur la bonne ou la mauvaise foi du titulaire grâce à la mise en œuvre de critères objectifs, à savoir la possession de la carte par le porteur au moment de l'opération frauduleuse, d'une part, et l'existence d'une contrefaçon telle que définie par la loi, d'autre part.

Cette rédaction est aussi protectrice que les précédentes pour le consommateur. Elle le décharge de toute responsabilité en cas d'utilisation frauduleuse des données de la carte lors d'un achat à distance. Elle l'exonère également de toute responsabilité en cas de fraude à la « *white plastic* » ou – il convient d'envisager l'hypothèse, même si dans la pratique elle n'a pas encore reçu d'application – à la « *Yescard* ». Dans ces derniers cas de figure, un code confidentiel pourra avoir été frappé par le fraudeur mais le titulaire légitime étant en possession physique de sa carte, sa responsabilité ne saurait être mise en œuvre.

Il convient d'observer que l'intervention du législateur pour protéger les consommateurs n'est pas inutile si l'on se réfère à la récente étude de l'association de consommateurs CLCV (consommation, logement et cadre de vie) sur les pratiques tarifaires des banques, qui montre, par exemple, qu'une grande banque française est susceptible de facturer 1.014 francs un usage de la carte bancaire au-delà des sommes disponibles sur le compte.

Un dispositif permettant à la France de faire figure de bon élève de l'Europe dans l'application de recommandations positives de l'Union européenne :

Les dispositions des articles 7 *ter* et 7 *quater* mettent en œuvre deux mesures essentielles de la recommandation de la Commission européenne du 30 juillet 1997 précitée.

Une étude récente, réalisée à la demande de la Commission européenne, a cherché à évaluer la transposition de cette recommandation dans les quinze pays membres de l'Union européenne (). Il est apparu très clairement qu'en ce qui concerne les droits et obligations des parties, la transposition de la recommandation est insuffisante (voir l'encadré de la page suivante).

Jusqu'à présent, le Danemark était le seul pays à avoir une législation conforme à l'ensemble des principes édictés par la recommandation. Sur le point spécifique des droits et obligations des parties au contrat, l'étude précitée notait expressément que la France (et les Pays-Bas) se distinguaient par une absence de réglementation.

Cette lacune est sur le point d'être comblée.

Un moyen de renforcer la confiance dans les cartes de paiement :

Plutôt que de favoriser une hypothétique irresponsabilité des porteurs de carte, les nouvelles dispositions que votre Rapporteur a tenu à faire adopter dans le cadre du projet de loi relatif à la sécurité quotidienne vont accroître la confiance des porteurs dans cet instrument de paiement.

Une étude réalisée, en 1999, pour le Parlement européen (), a constaté, en effet, que la confiance des consommateurs pourrait être supérieure si leur responsabilité était limitée, comme c'est le cas aux Etats-Unis où la franchise ne peut être supérieure à 50 dollars.

Cette question de la confiance constitue, par ailleurs, un préalable indispensable au développement du commerce électronique.

Après avoir traité de la question de la protection des consommateurs dans son rapport pour avis, votre Rapporteur souhaiterait justement examiner, dans le présent rapport d'information, les différents aspects de la relation entre commerce et cartes bancaires.

Les pages suivantes vont ainsi permettre d'étudier les dispositions du « contrat fournisseur » liant les commerçants au Groupement des cartes bancaires, le développement des porte-monnaie électroniques et les moyens techniques susceptibles de sécuriser les paiements sur Internet.

EXTRAITS DE L'ÉTUDE REMISE À LA COMMISSION EUROPÉENNE SUR LA TRANSPOSITION DE LA RECOMMANDATION

DU 30 JUILLET 1997

« *Les résultats de l'étude révèlent les problèmes suivants :*

1. Le but de la recommandation qui est d'offrir une transparence sur les conditions des transactions n'est pas atteint au moins sur quatre aspects :

– insuffisance de l'information fournie par les émetteurs aux titulaires ;

– mauvaise lisibilité de l'information (manque de clarté ou d'accessibilité) ;

– information fournie en temps inopportun ; et

– le niveau de respect varie suivant le type d'instrument de paiement électronique.

2. En ce qui concerne les droits et obligations des parties, la transposition de la recommandation est insuffisante sur les points suivants :

– l'obligation de limiter la responsabilité du titulaire après notification n'est pas respectée ;

– non respect de l'obligation de restreindre la responsabilité lorsque l'instrument de paiement électronique est utilisé sans présentation physique ou identification électronique ;

– absence d'uniformité parmi les Etats membres sur la notion de faute grave ;

– la période de préavis pour les modifications à apporter au contrat est souvent inférieure à un mois ;

– les dispositions relatives à l'annulation pour les montants indéterminés sont rares ;

– absence de dispositions relatives à la responsabilité de l'émetteur pour les transactions non exécutées ou mal exécutées.

3. Beaucoup d'émetteurs ne se conforment pas à la recommandation en ce qui concerne le respect des procédures de notification ou de responsabilité après notification en cas de vol ou perte :

– certains émetteurs n'expliquent pas la procédure de notification ;

– dans bien des cas, il n'existe aucune possibilité de prouver que la notification a été faite;

– certains émetteurs n'offrent que des possibilités d'accès limitées aux systèmes de notification, par exemple en restreignant les heures d'ouverture.

4. Dans la plupart des Etats membres, la charge de la preuve est placée sur le titulaire, ou au mieux pas mentionnée dans les dispositions contractuelles.

5. Les modes de résolution des litiges sont inadéquats :

– les contrats ne font souvent pas référence aux organes de résolution des litiges ni ne fournissent d'informations relatives aux personnes à contacter ;

– les organes de résolution des litiges sont souvent internes et il y a donc un manque d'indépendance ;

– les coûts liés à une action judiciaire sont élevés et la procédure d'une lenteur extrême ».

chapitre premier :

des relations apaisées entre les émetteurs de cartes

et les commerÇants

La plus « classique » et la plus répandue des utilisations de la carte de paiement est celle qui donne lieu à un paiement « en face à face » par l'intermédiaire d'un terminal de paiement électronique (TPE).

Il y a aujourd'hui, en France, 623.000 commerçants ou prestataires de services qui acceptent le paiement par cartes bancaires.

Ces commerçants sont liés aux banques émettrices de cartes par un contrat dit « contrat fournisseur », qui s'inspire d'un contrat type mis au point par le Groupement des cartes bancaires.

Par ce contrat, l'émetteur s'engage principalement à honorer les factures régulièrement payées par carte. Cette obligation revêt un caractère différent selon le montant de la dépense acquittée. Jusqu'à concurrence d'une certaine somme, dite « plafond garanti », l'émetteur assume à l'égard du fournisseur qui a respecté les instructions contenues dans son contrat, un engagement irrévocable de paiement (il ne saurait s'y soustraire en invoquant, par exemple, l'insolvabilité du porteur ou l'opposition de ce dernier, si celle-ci n'a pas été notifiée au fournisseur). En revanche, au-delà du plafond garanti, le remboursement du fournisseur n'a lieu que sous réserve d'encaissement auprès du porteur de la carte. Il s'agit donc, en ce cas, d'une simple avance sur facture, consentie par l'émetteur au fournisseur.

De son côté, le fournisseur souscrit également plusieurs engagements.

Il a, tout d'abord, l'obligation d'effectuer certaines formalités lors de chaque opération. Le commerçant est ainsi tenu de vérifier la date de validité de la carte et, éventuellement, l'apposition de la signature du client sur la facturette et sa conformité avec l'exemplaire apposé sur la carte (). Toute défaillance est de nature à engager sa responsabilité en cas d'utilisation frauduleuse de la carte par un tiers.

Le fournisseur est, par ailleurs, tenu de verser une commission, dite « commission interbancaire de paiement », sur le montant des factures acquittées au moyen de la carte. Il doit, en outre, posséder un TPE agréé par le Groupement des cartes bancaires et respectant un cahier des charges établi par ce dernier, ce qui conduit les commerçants à supporter d'importants investissements. Ces deux

dernières obligations ont donné lieu à des confrontations entre le commerce et la communauté bancaire, mais ces difficultés semblent, aujourd'hui, être atténuées : la première, à la suite de décisions contentieuses ; la seconde, du fait de la conclusion d'un protocole d'accord le 17 janvier 2001.

Il convient, d'ailleurs, de souligner que, selon une étude réalisée par la SOFRES du 8 au 17 octobre 1998 auprès de 800 responsables de magasins acceptant la carte « CB » en paiement, la carte « CB » est le moyen de paiement préféré de 55% des commerçants (contre 29% pour les espèces et 9% pour les chèques). Parmi les avantages qu'apporte la carte bancaire, la garantie de paiement est citée en premier lieu. Viennent ensuite la sécurité supplémentaire apportée par l'absence de manipulation d'argent liquide, la simplification de la gestion comptable et la diminution du temps de passage des clients aux caisses du magasin.

I.- le règlement par la voie contentieuse du conflit relatif à la commission interbancaire de paiement

Ce conflit a donné lieu à plusieurs interventions du Conseil de la concurrence. Il a, par ailleurs, eu des prolongements particuliers au secteur des grandes enseignes.

A.- le groupement des cartes bancaires sanctionné par le conseil de la concurrence

Ce ne sont pas moins de trois décisions du Conseil de la concurrence qui sont intervenues pour résoudre ce conflit.

Première décision

Le 15 septembre 1986, le Conseil national du commerce (qui porte, aujourd'hui, la dénomination de Conseil du commerce de France) a saisi le Conseil de la concurrence pour contester, notamment, une prétendue concertation des membres du Groupement des cartes bancaires sur le seuil des tarifications.

Dans sa décision n° 88-D-37 du 11 octobre 1988, le Conseil de la concurrence a constaté que le Groupement des cartes bancaires fixait lui-même le tarif de la commission que ses membres, lorsqu'ils agissent en qualité de banques de commerçants, versent, à l'occasion de chaque règlement effectué par carte bancaire, à ceux qui agissent en qualité de banques de porteurs de cartes. Cette commission, qui est destinée à la fois à rémunérer le risque afférent à la garantie de paiement assurée par la banque du porteur de la carte et à couvrir le coût des mesures collectives de sécurité, ainsi que les charges inhérentes au traitement de la transaction, était fixée à 0,8% du montant de la transaction avec toutefois un taux particulier de 0,4% pour les transactions effectuées chez certains grands distributeurs ; elle n'était pas applicable aux opérations « intrabancaires », qui ne font intervenir qu'une seule banque ou un seul groupe de banques.

Le Conseil de la concurrence a estimé que la fixation « concertée » de cette commission, dite alors d'« interchange », limitait la capacité des banques à négocier

avec les commerçants le taux de la commission que ces derniers leur versent à l'occasion de chaque transaction réglée par carte bancaire : le taux de cette commission, en principe fixé librement, se trouvait, dans les faits, rarement inférieur à celui de la commission d'interchange, dans la mesure où les banques des commerçants étaient « *incitées à pratiquer vis-à-vis de leur clientèle des taux de commission établis en fonction des montants qu'elles devront verser aux banques de porteurs* ».

Bien que la définition par les soins du Groupement des cartes bancaires de la commission d'interchange faussait le jeu de la concurrence, le Conseil l'a toutefois admise dans son principe, car elle lui est apparue nécessaire au bon fonctionnement du système de paiement par carte bancaire. Elle permettait, en effet, d'éviter que chacun des membres du Groupement soit contraint de négocier avec tous les autres un tarif particulier de commission.

Toutefois, relevant que le tarif de la commission d'interchange était applicable uniformément à tous les établissements financiers quelle que fût leur situation particulière, le Conseil a estimé non conformes « à l'objectif de progrès économique » les modalités retenues pour sa définition, au motif qu'elles empêchaient, en fait, les membres du Groupement « *de consentir à leur clientèle de commerçants des taux de commission reposant sur des critères objectifs et qui soient notamment en rapport avec les efforts des commerçants en vue de réduire les risques de fraude et d'utilisation abusive* ».

Le Conseil a donc enjoint au Groupement des cartes bancaires « *de mettre en application, au plus tard le 1er mai 1989, des modalités d'interchange fondées sur des critères objectifs tenant compte, en particulier, du degré de sécurité du paiement par carte bancaire dans les commerces* ».

Deuxième décision

Le Groupement des cartes bancaires a présenté au Conseil de la concurrence, le 29 mars 1989, les nouvelles modalités de calcul de la commission qualifiée désormais de « commission interbancaire de paiement ». L'examen de ces modalités a donné lieu à la décision du Conseil de la concurrence n° 89-D-15 du 3 mai 1989.

Sur recours du Groupement des cartes bancaires, la cour d'appel de Paris a, par un arrêt du 16 novembre 1989, annulé pour vice de forme cette décision. Mais, par un second arrêt, en date du 26 avril 1990, la cour d'appel de Paris juge également que telles qu'elles ont été constatées par la direction de la concurrence, de la consommation et de la répression des fraudes, les modalités de détermination de la commission interbancaire de paiement mises en œuvre par le Groupement des cartes bancaires ne sont pas conformes à l'injonction contenue dans la décision du Conseil de la concurrence du 11 octobre 1988.

D'après les considérants de cet arrêt, les modalités de calcul de la commission interbancaire de paiement doivent être conformes aux principes suivants :

– chacune des trois composantes de la commission doit être distinguée soit en part fixe, soit en pourcentage ;

– la part de la commission qui correspond aux charges de traitement ne doit pas être calculée en fonction du taux de fraude ;

– la part de la commission qui est afférente à la garantie de paiement doit pouvoir connaître « une progression continue et sans plafonnement ».

A la suite de l'arrêt du 26 avril 1990, le Groupement des cartes bancaires a adopté, pour le calcul de la commission interbancaire de paiement, de nouvelles modalités, applicables à compter du le 1er mai 1990.

La commission interbancaire de paiement comportait :

– un élément destiné à couvrir les charges qui sont inhérentes au traitement de toute transaction effectuée, quel que soit son montant ; il est fixé à 0,70 franc ;

– un élément destiné à couvrir le coût des mesures collectives de sécurité ; son montant est égal à 0,21% de la transaction ;

– un élément destiné à couvrir les dépenses que les banques des porteurs de carte sont amenées à engager au titre de la garantie de paiement qu'elles accordent aux commerçants. Son montant est également exprimé en pourcentage de la transaction, mais selon un taux variable, qui est le taux interbancaire de cartes en opposition (TICO), tel qu'il était calculé dans le système précédent, à ceci près que le fichier des oppositions pris en compte est celui de la veille et non du jour de la compensation.

Troisième décision

Dans une troisième décision n° 90-D-41 du 30 octobre 1990, le Conseil de la concurrence, saisi par le ministre de l'économie, des finances et du budget pour contrôler la conformité des dispositions adoptées par le Groupement des cartes bancaires avec les termes de sa décision n° 88-D-37 du 11 octobre 1988, a estimé que la structure de la commission interbancaire de paiement était conforme à l'injonction émise en 1988. En revanche, le Conseil de la concurrence a décidé de sanctionner le Groupement des cartes bancaires, à raison, d'une part, de l'inexécution de l'injonction précitée pendant la période allant du 1er mai 1989 au 30 avril 1990 et, d'autre part, de la prise en compte du fichier des oppositions de la veille du jour de la compensation des opérations interbancaires, alors qu'il résulte de l'arrêt de la cour d'appel du 26 avril 1990 qu'un décalage par rapport au jour de la compensation réduit l'incidence de la fraude sur la partie variable de la commission (le choix du jour J-1 ne pouvait donc être regardé comme répondant à la condition d'objectivité).

Une sanction pécuniaire de six millions de francs a ainsi été infligée au Groupement des cartes bancaires.

Depuis, les juridictions n'ont plus été appelées à se prononcer et, lors de leur audition par votre Rapporteur, les représentants du Conseil du commerce de France ont estimé que les niveaux de tarification de la commission interbancaire de paiement (entre 0,4% et 1,4% de la transaction) pouvaient être qualifiés d'« acceptables ».

Il convient effectivement de souligner que les taux appliqués sont sensiblement inférieurs à ceux constatés chez certains de nos partenaires européens. Ils s'élèvent, en effet, à 4% en Espagne et au Portugal.

Par ailleurs, si l'on rappelle qu'en 1999 les paiements réalisés avec une carte bancaire « CB » ont atteint 883 milliards de francs, on perçoit qu'un faible pourcentage de commission peut néanmoins concerner des sommes très importantes (de l'ordre de 7 à 10 milliards de francs).

b.- l'échec de la fronde des grandes enseignes

Comme cela vient d'être indiqué, le pourcentage de la commission interbancaire de paiement varie fortement ; le plus faible bénéficiant aux grands distributeurs.

Cela n'a pas empêché ces derniers d'être les plus offensifs à l'encontre du Groupement des cartes bancaires.

Une première réaction a pris la forme de la création de cartes spécialisées (telles que, par exemple, les cartes *FNAC* ou *Carrefour*), qui ont permis, en fait, aux enseignes émettrices de mieux négocier le taux de leur commission interbancaire de paiement.

Une autre stratégie a été mise en œuvre par les établissements *Leclerc*, qui, en septembre 1987, avaient bâti un système parallèle à celui du Groupement des cartes bancaires, afin de « court-circuiter » ce dernier, tout en continuant de bénéficier des avantages de l'affiliation au Groupement (consultation des fichiers, notamment).

La méthode avait nécessité la création d'un « club » et, surtout, la connivence de certaines banques, pourtant adhérentes du Groupement des cartes bancaires.

Le client pouvait continuer à régler ses achats par carte bancaire, mais il autorisait le « club » – qui lui fournissait certains services accessoires (petit crédit, assurance décès-invalidité, voyages à tarif avantageux, réduction pour les spectacles…) – à prélever directement sur son compte bancaire le montant des achats réalisés par carte. Ce circuit raccourci permettait à *Leclerc* d'accomplir à moindre frais le travail réalisé, en principe, par le Groupement des cartes bancaires.

Cette tentative a, cependant, échoué. Le Groupement des cartes bancaires a considéré que les établissements concernés ne respectaient pas les obligations

imposées par le « contrat fournisseur » et, comme ce dernier lui en donne le droit, il a résilié de façon unilatérale leur contrat, empêchant l'usage des cartes « CB » dans ces établissements. Cette résiliation a été jugée légitime par un arrêt de la cour d'appel de Paris du 30 juin 1988 et par la chambre commerciale de la Cour de cassation, dans un jugement du 27 février 1990.

II.- le protocole d'accord du 17 janvier 2001

Le second point de discorde entre les commerçants et les émetteurs de cartes portait sur l'importance des investissements supportés par les commerçants.

L'accord, signé le 17 janvier dernier, répond à la demande de concertation émanant du secteur du commerce. Il fixe le calendrier et les modalités techniques de la modernisation et du renforcement sécuritaire des TPE.

a.- une réponse à la demande de concertation des commerçants

Le commerce est fortement impliqué dans le système carte bancaire, puisque, dans la majorité des cas, les commerçants sont propriétaires de leur(s) TPE, ce qui constitue une situation quasi unique au monde. Cette implication l'a conduit à supporter la charge de lourds investissements.

Dans un premier temps, les commerçants français ont accepté d'entreprendre la mutation massive de la technique « piste magnétique » à la technique « puce ».

Actuellement, ils se trouvent confrontés à une série d'évolutions techniques, nécessitant des investissements d'un montant supérieur à 6 milliards de francs.

Il convient, en effet :

– d'adapter les TPE au passage à l'euro ;

– d'élever, avant la fin de l'année, le niveau sécuritaire des équipements, grâce au contrôle impératif de la valeur d'authentification sécurisée (dite « VS ») ;

– de permettre, en application de la charte relative à la sécurité des cartes de paiement signée le 22 février 2001 par le Conseil du commerce de France, l'impression de tickets faisant apparaître des numéros tronqués () ;

– de migrer, avant le 1er mai 2003, vers la version CB 5.2, intégrant le standard international « EMV » ().

Ces divers investissements apparaissent absolument nécessaires, puisque, comme votre Rapporteur l'avait souligné dans son rapport pour avis sur le projet de loi relatif à la sécurité quotidienne, les TPE constituent le maillon faible de la chaîne sécuritaire. Leur mise à niveau est donc un aspect fondamental de toute évolution du

système de paiement par cartes.

Il n'en demeure pas moins que cette charge a parfois été mal acceptée par les commerçants, qui ont eu le sentiment :

– d'une part, de payer le coût d'erreurs dont ils ne sont pas responsables : la modification des tickets émis, en particulier, est perçue comme un effort destiné à résoudre un problème spécifique aux entreprises de vente à distance (effort d'autant plus pesant, qu'il pourrait faciliter la répudiation des transactions des clients américains) ;

– d'autre part, de se voir imposer ces évolutions sans pouvoir faire valoir leur point de vue.

Lors des travaux réalisés, à compter d'avril 2000, par le groupe de travail rattaché au Conseil national de la consommation, chargé de dresser un état des lieux de la sécurité des cartes bancaires, le Conseil du commerce de France s'est ainsi livré à une analyse du « contrat fournisseur », d'où il ressortait nettement une demande de concertation accrue avec les banques.

Il était notamment reproché au Groupement des cartes bancaires de modifier « de manière permanente » les cahiers des charges. A titre d'exemple, le Conseil du commerce de France soulignait que le logiciel CB 5.1 a été modifié à huit reprises en un an et demi. Il faisait également mention des problèmes liés au téléchargement (blocage du TPE plusieurs jours ou encore effacement des applications des cartes privatives).

Cette demande d'une meilleure visibilité des commerçants sur le rythme d'évolution des normes a été entendue et s'est traduite par la signature, le 17 janvier 2001, du « protocole d'accord pour le déploiement de la version CB 5.2 du système de paiement par cartes bancaires », engagement souscrit par le Groupement des cartes bancaires et le Conseil du commerce de France.

B.- une mise en œuvre concertée des investissements à entreprendre

Par cet accord, le Groupement des cartes bancaires et le secteur du commerce s'engagent sur le calendrier et les modalités du passage du système actuel (standard BO') au standard international EMV, ces évolutions constituant le programme CB 5 de la communauté bancaire « CB ».

Le calendrier prévoit une étape intermédiaire, s'achevant avant la fin 2001, visant à renforcer le niveau de sécurité des équipements et à assurer le passage à l'euro. La migration vers le programme CB 5 devra être achevée le 1er mai 2003.

Le Groupement des cartes bancaires s'est, par ailleurs, engagé à figer les spécifications CB 5, dans la version définie en octobre 2000, jusqu'à la fin 2002.

Surtout, une collaboration plus étroite des différents acteurs est prévue, grâce à la mise en place d'un comité de suivi, coprésidé par le Conseil du commerce de France et par le Groupement des cartes bancaires, qui devrait permettre – selon les termes d'un document remis par le Groupement à votre Rapporteur – de « *piloter conjointement le devenir de la monétique CB* ».

Après cet examen des relations « traditionnelles » entre le commerce et les cartes bancaires, il importe de s'intéresser aux mutations en cours des systèmes de paiement électronique. Ces évolutions concernent, d'une part, la monétique « hors ligne » sur les réseaux propriétaires bancaires, par l'intermédiaire du porte-monnaie électronique et, d'autre part, le développement de systèmes « en ligne » sur les réseaux non propriétaires, tel qu'Internet.

chapitre II :

LE PORTE-MONNAIE ÉLECTRONIQUE :

DES EXPÉRIENCES MULTIPLES N'AYANT PAS encore DÉPASSÉ

LE STADE EXPÉRIMENTAL

La carte bancaire n'est pas obligatoirement le moyen de paiement le mieux adapté pour l'ensemble des transactions. Il semble ainsi possible de déterminer trois niveaux d'intervention pour les systèmes de paiement électronique, ayant comme point commun la carte à puce :

– les transactions mettant en jeu de gros montants peuvent être réalisées par des systèmes à clef publique (PKI) () ;

– la carte bancaire peut être utilisée pour les montants moyens ;

– en ce qui concerne les petites dépenses, qui ne justifient pas la lourde procédure de la carte de paiement, le porte-monnaie électronique (PME) apparaît comme une solution pertinente.

I.- Un instrument adapté aux paiements de petits montants

Le PME peut être défini comme « *une carte prépayée multi-commerçant conçue principalement pour le commerce de détail et le paiement de petits montants (quelques francs), pour lequel les chèques et les cartes bancaires sont inadaptées en raison des coûts marginaux de transactions* () ».

Il s'agit donc d'une réserve de fonds préalablement constituée sur une carte à puce. Cette réserve est généralement effectuée par le transfert de monnaie scripturale sur le PME *via* des distributeurs automatiques de monnaie électronique ou d'autres bornes équivalentes. Cette réserve prépayée est débitée après chaque paiement et créditée ensuite au commerçant.

La sphère potentielle des paiements susceptibles d'être effectués au moyen d'un PME recouvre les paiements inférieurs ou égaux à 100 francs. Le PME est donc destiné à se substituer aux pièces et billets en circulation, qui constituent des moyens de paiement coûteux (gestion des encaisses, manipulations, probabilités de contrefaçon).

Le PME possède de nombreux atouts qui auraient dû favoriser son développement.

– Pour le porteur :

Le PME présente, tout d'abord, un caractère pratique, car il dispense le consommateur de détenir des espèces encombrantes.

Il s'agit, par ailleurs, d'un instrument de paiement ne soulevant pas de difficultés particulières en ce qui concerne la sécurité. En effet, contrairement à la carte bancaire, qui constitue un instrument d'accès au compte bancaire *via* des réseaux de télécommunications, le PME ne requiert aucune autorisation de l'institut émetteur pour procéder au paiement. Il ne donne pas accès au compte courant du titulaire, ce qui signifie qu'en cas de perte ou de vol, le préjudice subi par le porteur n'est pas plus important que celui qu'il supporterait en cas de perte ou de vol d'un porte-monnaie contenant des espèces.

Par ailleurs, le PME pourrait permettre aux exclus du monde bancaire traditionnel de disposer d'un instrument performant. « *Notons que les Etats-Unis ont perçu cet intérêt puisque dans certains Etats américains, le PME sert de support à l'aide gouvernementale à destination des particuliers. Dans le même ordre d'idée, le PME portugais a été adopté par des agents qui ne disposaient pas de compte bancaire actif* () ». Pour la France, on peut imaginer qu'il vienne compléter la liste des services bancaires de base fixée par le décret n° 2001-45 du 17 janvier 2001, pris pour l'application de l'article L. 312-1 du code monétaire et financier.

– Pour le commerçant :

De ce point de vue, le PME permet surtout d'éviter les manipulations d'espèces, ce qui induit un gain de temps aux caisses et diminue les risques.

– Pour les banques :

Le PME apparaît à la communauté bancaire française comme une occasion de rompre avec la logique des moyens de paiement gratuits et de faire accepter au public l'idée d'une facturation des moyens de paiement.

Compte tenu des divers avantages du PME, on a assisté à un foisonnement de projets ces dernières années.

II.- de multiples initiatives en europe

A la fin de 1997, on estimait que sept millions de PME étaient déjà diffusés dans trente-quatre pays au monde.

En ce qui concerne l'Europe, un récent rapport () estime à 22 le nombre des initiatives développées en la matière.

Ces divers projets ont notamment été analysés par un rapport de l'Observatoire européen pour la science et la technologie (ESTO) (), qui constate d'importantes différences entre le dispositifs et qui observe que ces instruments sont

encore à un stade expérimental.

Quelques initiatives méritent d'être signalées :

– en Finlande, le PME *avant* a été le premier à être diffusé à une échelle nationale, en décembre 1992. Il serait utilisé par 250.000 consommateurs ;

– au Danemark, le PME *danmønt* est utilisable sur le plan national depuis 1993. 500.000 cartes ont donné lieu, en 1997, à 5,5 millions de transactions dans 6.000 points de vente, pour un montant moyen de 1,35 euro. Cette technologie a été exportée dans plus de 20 pays ;

– en Allemagne, le PME *geldkarte* est susceptible d'être utilisé sur l'ensemble du territoire depuis 1997. Toutefois, si près de 45 millions de cartes ont été distribuées, 500.000 seulement ont été utilisées en 1998, pour réaliser 13,6 millions de transactions d'un montant moyen de 6,5 euros ;

– en Belgique, le PME *proton*, en usage depuis 1996, connaît un succès non négligeable. 7 millions de cartes acceptées par 50.000 terminaux permettent d'effectuer 70 millions de transactions par an, pour un montant moyen d'environ 40 francs. Les commerçants acceptant cette carte doivent s'acquitter d'une commission de 0,7% des montants et le porteur paie sa carte moins de 25 francs (cette carte étant rechargeable).

Ces diverses initiatives, les plus avancées en Europe, avec également le PME portugais *multibanco electronique purse*, autorisent à formuler plusieurs remarques :

– en premier lieu, ces PME n'ont guère dépassé le stade expérimental. Même *proton*, qui peut paraître fortement diffusé, ne vise pas une part de marché supérieure à 5% des paiements de petits montants. Cet objectif est d'ailleurs difficile à atteindre et certains fabricants d'automates (des distributeurs de boissons notamment), refusent d'équiper leurs appareils à cause du coût de cet investissement ;

– ensuite, ces produits privilégient la simplicité et le pragmatisme ; en particulier, les PME ne peuvent traiter que la devise du pays ;

– enfin, les pays concernés (Finlande, Danemark, Belgique, Portugal) sont des pays de taille moyenne où les cartes bancaires fonctionnent en mode « en ligne » (en France, moins de 10% des opérations font l'objet d'une autorisation), ce qui pénalise l'usage des cartes bancaires pour de petits montants, en raison des coûts de télécommunications.

Cette dernière remarque explique peut-être le faible intérêt que les banques françaises ont longtemps eu à l'égard du PME.

III.- une expérimentation tardive en France

La France, qui est un *leader* incontestable dans le domaine des cartes à puce, a tardé à développer le PME. Le rapport précité de l'Observatoire européen ESTO émet l'hypothèse que ce retard pourrait être expliqué notamment par le fait que la carte bancaire française peut être utilisée dans les parcmètres ou les cabines téléphoniques, c'est-à-dire des cibles privilégiées du PME.

Après avoir refusé, en 1994, de soutenir un projet présenté par La Poste, les banques françaises ont finalement accepté le principe du PME, mais elles l'ont fait en ordre dispersé et trois projets ont vu le jour :

– *monéo* : en novembre 1997, le Groupement des cartes bancaires a annoncé la création de la société financière du porte-monnaie électronique, chargée d'étudier les conditions de lancements du PME en France. Lors de l'été 1998, il a été décidé de se rapprocher de la solution allemande, *geldkarte*. Le PME *monéo* a fait l'objet d'une expérimentation à Tours avec 1.500 commerçants et 500 automates ;

– *modéus* : ce PME soutenu par La Poste, la SNCF, la RATP, les caisses d'épargne, les banques populaires et la Société générale présentait la particularité de développer la technique du « sans contact », afin de coupler les fonctions billétiques aux fonctions monétiques, ce qui correspond à une demande des sociétés de transport. Des tests ont été menés à Noisy-le-Grand et à la gare Montparnasse ;

– *mondex* : à la fin de 1998, un troisième projet de PME soutenu par le Crédit mutuel a vu le jour. Ce projet visait à mettre en œuvre le système *mondex* d'origine britannique, qui présente la spécificité d'autoriser des transferts de valeur de carte à carte. Une opération pilote a été engagée à Strasbourg.

En mars 2000, le paysage du PME français a été transformé, du fait de la fusion de *monéo* et *modéus*. Le PME développé par la communauté bancaire conserve l'appellation de *monéo*. Tout récemment, un plan de déploiement ambitieux a été annoncé : le système *monéo* devrait équiper progressivement l'ensemble des cartes bancaires, au fur et à mesure de leur renouvellement, ce qui permettrait d'en généraliser son utilisation d'ici à 2004.

Cette nouvelle carte mixte devrait offrir au porteur le choix d'effectuer des dépenses de n'importe quel montant : soit à travers l'application *monéo* jusqu'à 50 francs, soit – au choix du client – à travers *monéo* ou la carte bancaire entre 50 et 200 francs et, enfin, par carte bancaire au-delà de 200 francs.

Des bornes de rechargement du PME seront disponibles en libre-service dans les agences bancaires et chez les commerçants.

Le développement du PME *monéo* devrait, en outre, être facilité par la cessation du projet *mondex*, annoncée en juin dernier.

Il n'en demeure pas moins qu'« *il semble peu vraisemblable que le PME sur une carte à micro-processeur puisse, en tant que tel, atteindre le seuil de*

rentabilité économique : les investissements à réaliser sont importants. Les réticences des commerçants élevées et la valeur ajoutée pour les consommateurs modeste () ».

Le simple couplage avec des fonctions de billétique et de lecture à distance (le « sans contact ») apparaît aléatoire à la plupart des experts, en raison notamment de la diversité des systèmes de gestion des réseaux de transport. La viabilité économique nécessitera sans doute d'intégrer le PME à un ensemble de fonctionnalités complémentaires : sécurité (gestion des clés et des certificats), gestion de portefeuille mobilier ou non…

On pourrait être tenté également de préconiser l'utilisation du PME pour opérer des paiements en ligne sur Internet, comme cela est déjà possible avec les porte-monnaie finlandais (*avant*) et suédois (*cash*). Toutefois, le PME conçu pour le commerce traditionnel semble inadapté au commerce électronique « *en raison de l'architecture des réseaux, des protocoles et des besoins de sécurité* () ».

CHAPITRE III :

LE BESOIN DE SÉCURISATION DU COMMERCE ÉLECTRONIQUE

Même si le commerce électronique ne saurait être défini par la possibilité d'effectuer un paiement en ligne sur Internet, il faut bien reconnaître que cette activité n'a pas connu le développement escompté, en raison surtout du manque de confiance des utilisateurs. Il existe pourtant de très nombreux systèmes permettant de sécuriser les transactions sur Internet, qui ne font pas tous appel, d'ailleurs, à la carte bancaire.

I.- le commerce Électronique ne doit pas être confondu avec le paiement en ligne sur internet

A.- internet n'est pas le seul vecteur du commerce Électronique

La notion de commerce électronique ne doit pas être confondue avec celle de commerce sur Internet. De nombreux autres réseaux peuvent être utilisés pour réaliser des opérations commerciales par voie électronique.

Cinq grandes catégories de services-réseaux numériques peuvent ainsi être distinguées () :

– les services à valeur ajoutée (SVA), dont les archétypes sont les systèmes de réservation aérienne et les systèmes d'informations et de transactions financières, tel *Reuters*. Ces systèmes sont fermés, dans la mesure où seuls les abonnés peuvent y accéder ;

– le vidéotex, dont l'exemple le plus connu est le *Minitel*. En matière de commerce résidentiel, ce dernier demeure, en France, de loin, le premier media du commerce électronique (7 à 8 milliards de francs d'achats, contre 500 millions de francs environ pour les achats sur Internet) (). Son succès doit beaucoup, d'une part, à la diffusion gratuite des terminaux et, d'autre part, à l'invention du principe tarifaire du « kiosque », par lequel l'opérateur de réseaux prélève, pour le compte du fournisseur de services informationnels, des « minutes » de communication qu'il lui reverse ensuite. De là même façon, en Allemagne, le système *Btx* (désormais appelé « *T-Online* ») est fortement utilisé ;

– les échanges de données informatisés (EDI), dont les archétypes sont, en France, le système *galia* d'échange d'informations entre les constructeurs automobiles et leurs partenaires et le système *gencod* utilisé dans la grande

distribution. Ces EDI ont été développés à partir de la fin des années 1980. En 1999, alors que seulement 8% des entreprises industrielles françaises avaient des commandes en ligne sur Internet (même si elles étaient environ 24% à y diffuser de l'information), elles étaient près de 44% à réaliser des échanges EDI avec leurs partenaires (36%), l'administration (15%) ou entre établissements (14%). En termes de volumes d'affaires, dans le cas de la France, en 1999, on estimait à 800 milliards de francs le volume des échanges commerciaux sur EDI, contre 7,3 milliards de francs de chiffre d'affaires en « *business to business* » (B2B) sur Internet ;

– les places de marché, qui associent les technologies de l'EDI, des serveurs Internet sécurisés et de l'extranet (capacité de créer des réseaux virtuels à accès contrôlé sur Internet) pour organiser de véritables marchés virtuels. Les abonnés au système peuvent, de manière anonyme et sécurisée, envoyer des propositions commerciales sur le réseau auquel sont connectés l'ensemble des clients et fournisseurs potentiels. Ces derniers répondent à ces propositions et une sélection est opérée. Pour le moment, la plupart des systèmes sont encore en phase de test ;

– les serveurs Internet sécurisés : l'innovation d'Internet en matière de commerce électronique tient essentiellement aux technologies de l'« *Internet Protocol* » (IP). L'IP est un protocole de communication permettant l'interopérabilité de réseaux hétérogènes. Il fait de l'ensemble des réseaux physiques disponibles à travers le monde un seul réseau logique. La technologie du web, quant à elle, fournit un système d'adressage et de présentation normalisée de l'information.

Par ailleurs, pour ce qui concerne le grand public, les réseaux de télévision numérique et les réseaux de communication avec les mobiles constituent des médias appelés à supporter de nombreuses applications de commerce électronique.

Tous ces moyens ne doivent pas être considérés comme des substituts mais comme des compléments. Il n'en reste pas moins vrai qu'Internet est porteur d'un approfondissement du mouvement d'électronisation du commerce.

B.- Le paiement en ligne ne caractérise pas le commerce électronique

Une transaction comporte plusieurs opérations et le paiement ne constitue que l'une d'entre elles. En fait, plusieurs définitions du commerce électronique sont possibles, qui peuvent s'organiser en gigogne () :

– une définition « large » pourrait être : constitue une activité de commerce électronique, toute activité d'échange générant de la valeur pour l'entreprise, ses fournisseurs ou ses clients, effectuée sur des réseaux. Cette définition inclut l'information d'avant-vente, la relation clientèle, voire les échanges purement financiers (paiement de factures…). Elle présente l'avantage d'être plus juste d'un point de vue théorique, et l'inconvénient de se prêter assez difficilement à la mesure ;

– une définition « restreinte » couvre l'ensemble des activités commerciales conduisant à des transactions amorcées (commande ou intention de commande) en ligne. Il doit y avoir transaction, donc génération de chiffre d'affaires, mais pas nécessairement paiement ;

– une définition « étroite » se limite aux transactions engagées et conclues en ligne, paiement compris. Elle rend particulièrement mal compte des échanges entre les entreprises.

Il convient de noter que, selon la définition fournie par l'OCDE, une entreprise effectue du commerce électronique sur Internet, si elle est présente sur le réseau de télécommunications par le moyen d'un site web qui offre la possibilité de passer une commande en ligne. Le paiement et la livraison peuvent être effectués de différentes manières. Cette définition rejoint la définition « restreinte » de la typologie dressée précédemment.

Dès lors, dans la grande majorité des cas, le commerce électronique sur Internet ne repose, aujourd'hui, que sur l'électronisation de la recherche d'un partenaire. La négociation et la prise de commande en ligne demeurent rares. En termes économiques, dans le cadre du « *business to consumer* » (B2C), les fonctions *ex ante* prédominent. Le seul segment marqué par une offre significative de services orientés vers la gestion *ex post* de la relation est le secteur bancaire et financier (le courtage en ligne représente environ 45% du courtage aux Etats-Unis).

De façon significative, on estime que, dans le cas du marché automobile américain, par exemple, moins de 1% des transactions sont réalisées en ligne, mais les deux tiers des transactions sont préparées sur le web, qui sert aux acheteurs à s'informer sur l'offre et sur les revendeurs. En France, en 2000, on considérait que 16% des internautes avaient effectué une commande en dehors de la « toile », mais à partir d'informations relevées sur Internet ().

Les moyens de paiement traditionnels, comme le chèque ou le virement, restent parfaitement utilisables pour payer les biens commandés en ligne. Il semblerait même, selon une étude citée par un rapport du ministère de l'économie, des finances et de l'industrie (), que les paiements par chèque représentent les deux tiers des montants des paiements d'achats sur Internet, en France.

Le paiement en ligne est néanmoins une facilité qui peut soutenir le développement du commerce électronique. Or, la croissance de ce dernier ne correspond pas aux prévisions.

II.- Une forme de commerce encore marginale

« *Le commerce électronique demeure insaisissable, relevant encore de nos jours plus de la chronique d'une technologie naissante que de celle d'un nouveau canal de distribution à exploiter* » ().

Ce caractère insaisissable ressort notamment de la difficulté d'obtenir des

chiffres fiables sur le commerce électronique. Les chiffres disponibles sont majoritairement des prévisions, plutôt que des évaluations, et sont peu compatibles entre eux (à titre d'exemple, les estimations du commerce électronique aux Etats-Unis, fournies pour les années 1995-1997, varient de 70 millions à 24 milliards de dollars). Les taux de croissance estimés divergent également fortement d'un organisme à l'autre.

A.- Un développement inférieur aux prévisions

En tout état de cause, le commerce électronique est encore peu développé. Même dans les pays qui ont été précoces dans la mise en place des nouvelles technologies de l'information et de la communication, il reste marginal. Selon le département du commerce américain, il représente 0,68% du commerce de détail dans ce pays au premier semestre 2000. La Corée du sud est le pays *leader* dans ce domaine, mais avec un taux de 1,1% en juin 2000.

La plupart des sites de commerce électronique n'ont pas encore démontré leur viabilité économique (tous, y compris les plus connus, tel *Amazone*, perdent de l'argent).

En ce qui concerne la France, le développement s'est révélé particulièrement lent. Satisfaits des performances du *Minitel*, les Français sont restés très prudents face à Internet. Même si le taux de croissance du commerce électronique est désormais équivalent à celui constaté chez nos partenaires européens, la France n'a pas encore comblé son retard : il y a dans notre pays considérablement moins de sites web qu'en Grande-Bretagne ou en Allemagne (moins de 1% du total mondial des sites web sont en France).

Un état des lieux a été dressé récemment par l'INSEE (). Il en ressort qu'en 1999, environ deux cents entreprises du commerce de détail proposaient leurs services aux particuliers par Internet et que leurs échanges couvraient moins de 0,1% du chiffre d'affaires total du commerce de détail, soit un peu plus d'un milliard de francs. Même si la croissance est rapide (en 1998 le chiffre d'affaires n'était que de 500 millions de francs et, au premier semestre 2000, les ventes ont dépassé celles de l'ensemble de l'année 1999), il convient de souligner qu'actuellement ce chiffre d'affaires est, en gros, équivalent à celui de trois supermarchés.

Il importe de noter que tous les chiffres précités concernent les applications grand public du commerce électronique, que, dans ce domaine où la francophonie a peu de place, on aime à qualifier de *business to consumers* (B2C). Les applications professionnelles (dites B2B (), *business to business*), qui renvoient aux transactions interentreprises, représentent des volumes d'échanges beaucoup plus importants (huit à dix fois supérieurs).

Marginal, le commerce électronique n'est plus anecdotique : en 2000, 30% du chiffre des ventes d'une société comme *General Electric* se sont faits par Internet.

Surtout, il constitue un formidable marché potentiel : si l'on tient compte des 300 millions de téléphones cellulaires en service, il n'est pas déraisonnable de penser que les 150 millions d'internautes actuels, dans l'Union européenne, pourraient être 500 millions d'ici 2005.

S'ajoute à cela le passage à l'euro, même si l'impact de cet événement est difficile à évaluer sur le développement du commerce électronique transfrontalier.

B.- un problème certain de besoin de sécurité

Diverses raisons peuvent être avancées pour expliquer le succès relatif actuel du commerce électronique.

Il semble qu'il faille écarter toute explication liée à l'équipement des ménages en accès à Internet. Le rapport précité de l'observatoire européen ESTO constate que le commerce électronique n'a pas connu un développement plus sensible dans les pays les mieux équipés (dans les dix pays de l'Union européenne étudiés par ce rapport, le taux des équipements personnels d'accès à Internet varie de 4% à 33%).

Ainsi, en Finlande – pays qui, avec la Suède, dispose du taux de connection le plus élevé au monde – le commerce électronique n'a pas connu une croissance supérieure à celle constatée par ailleurs.

Une première explication des freins au développement du commerce électronique met en cause les entreprises. Elles n'ont pas forcément eu conscience de l'émergence de ce nouveau marché et, de plus, n'ont pas toujours compris suffisamment que cette activité nécessitait d'adapter les produits et la logistique. En outre, l'absence d'un cadre légal approprié à Internet (en particulier la difficulté d'appliquer les clauses contractuelles usuelles) a pu les retenir d'intervenir sur ce marché.

Ce problème juridique est également avancé pour expliquer la « timidité » des consommateurs. Le rapport précité « S*tudy on electronic payment systems* », réalisé pour le Parlement européen, estime ainsi que l'avance des Etats-Unis en ce domaine suggère que l'existence d'une réglementation protégeant le consommateur est peut-être un point clef de l'essor du commerce électronique. Les dispositions figurant dans le projet de loi relatif à la sécurité quotidienne répondent donc à une nécessité non seulement juridique, mais aussi économique.

Du côté des consommateurs, on invoque également des raisons tenant au coût des télécommunications, aux obstacles culturels (d'ordre linguistique et générationnel).

Surtout, même si les experts peuvent être divisés sur ce point, toutes les enquêtes font apparaître une exigence de sécurisation du commerce électronique.

Il faut bien comprendre, en effet, que dans le monde du commerce

électronique, un client réputé réel achète un bien censé exister à un marchand virtuel. Confiance et sécurité sont donc perçues comme aléatoires et l'incertitude réside dans le cœur même de l'acte d'achat, comme l'attestent différentes enquêtes :

– selon l'INSEE, trois détaillants sur quatre considèrent la sécurité sur Internet comme un frein au développement du commerce électronique ;

– selon une étude du cabinet Raffour Interactif, 72% des internautes Français se méfient du commerce électronique. Plus précisément, 46% des internautes interrogés se disent « un peu plus méfiants » et 26% « beaucoup plus méfiants », tandis que 26% s'affirment sans méfiance et 2% sont sans opinion. Interrogés sur ce qu'ils considèrent comme un « frein » à la décision d'achat sur Internet, 67% des internautes évoquent la sécurité des modes de paiement, 50% le surcoût lié à la livraison, 47% la réutilisation possible des données personnelles, 44% leurs doutes sur le service après-vente, 25% de délai de livraison, et 23% l'absence de relation commerciale physique.

Certains spécialistes considèrent que cette méfiance est davantage un problème psychologique qu'une appréciation réaliste des risques. Il n'en demeure pas moins qu'elle a des effets concrets :

– les ventes se concentrent sur des secteurs bien identifiés : voyages, librairie, compact disques, micro-informatique et logiciels, services financiers. Il s'agit donc de biens et services fortement standardisés et peu complexes dont les caractéristiques sont susceptibles d'être décrites *via* une interface relativement pauvre. Selon l'INSEE, le montant moyen de la plupart des commandes, en France, est de l'ordre de 500 francs ;

LA STRUCTURE DU COMMERCE B2C EN FRANCE ET AUX ETATS-UNIS EN 1999				
Secteur	**France**		**Etats-Unis**	
	Montant ***(en millions de francs)***	**% du total**	**Montant** ***(en millions de dollars)***	**% du total**
Voyage – transport – hôtellerie	620	47,18	7.798	38,33
Informatique (matériel et logiciel)	312	23,74	4.455	21,89
Produits culturels (livres-musique-vidéo)	137	10,43	2.376	11,67
Habillement	5	0,38	1.620	7,96
Fleurs, cadeaux	15	1,14	656	3,23
Alimentaire, boisson	33	2,51	513	2,52
Santé, beauté	-	-	509	2,50
Mobilier, électroménager	25	1,90	446	2,19
Billetterie	7	0,53	300	1,47
Jeux	2	0,15	253	1,24
Généralistes (VPC, Distribution, Galerie)	92	7,00	-	-
Divers	66	5,02	1.418	6,97
Total	**1.314**	**100**	**20.344**	**100**

Source : Eric Brousseau, Economie et statistique n° 339-340, précité, d'après Benchmark Group, 2000 pour la France

(Enquête réalisée auprès des « 75 sites marchands français les plus actifs ») et

Forester Research, 2000, pour les Etats-Unis.

– certaines banques, ayant classé le commerce électronique dans les activités à risque, refusent de délivrer, à de nouvelles entreprises, souhaitant se positionner dans le commerce électronique, le numéro de compte de commerçant qui permettrait, à leurs clients, d'utiliser la carte bancaire pour payer les biens ou services commandés.

Il apparaît donc que le commerce électronique ne se développera que si acheteurs et vendeurs peuvent se faire mutuellement confiance. Le principal enjeu réside dans le développement de systèmes de paiement en ligne capables de gérer de manière fiable un grand nombre de micro-paiements pour les usages du grand public.

III.- des moyens de sécurisation foisonnants ne mettant pas obligatoirement en œuvre la carte à puce

On assiste actuellement à une profusion d'idées et de réalisations, ce créneau semblant particulièrement inspiré les inventeurs. On recenserait ainsi plus de trois cents modes de paiement prévus pour Internet.

Cette profusion de dispositifs, souvent éphémères, peut susciter la perplexité et l'attentisme des usagers. En tout état de cause, elle rend complexes les tentatives de classification effectuées par les économistes.

Certains distinguent deux grandes familles d'instruments de sécurisation : ceux destinés aux paiements de petits montants et ceux pour les paiements d'opérations commerciales courantes.

Le rapport du groupe technique restreint ayant participé aux travaux engagés sous l'égide du Conseil national de la consommation a, quant à lui, opéré une répartition entre les solutions totalement « en ligne » et les solutions mixtes.

Il est également possible d'identifier deux grandes classes : la première est conçue comme une extension de la monnaie fiduciaire et scripturale (le transfert de monnaie sur le réseau est effectué à partir d'un moyen de paiement scriptural articulé autour d'un compte bancaire) ; la seconde est envisagée comme un substitut soit au compte bancaire, soit au numéraire.

La typologie la plus fouillée distingue cinq classes de systèmes : la monnaie électronique, les protocoles sécurisés, les systèmes privés de compensation, les systèmes notariés en compte et les systèmes privés de fidélisation.

Compte tenu de l'objet du présent rapport d'information, il paraît plus opportun de s'en tenir à une séparation entre les systèmes de paiement impliquant la carte bancaire et les autres.

Ces derniers ne peuvent donner lieu, ici, à une analyse exhaustive. On se bornera à évoquer quelques solutions intéressantes.

A.- le virement par banque à distance

En Finlande, pays que l'on a déjà cité pour l'importance du nombre d'utilisateurs d'Internet, le système le plus couramment utilisé met en œuvre le virement à distance.

En pratique, lorsqu'un consommateur passe une commande sur un site marchand web, il lui indique les coordonnées de sa banque. Le site marchand dirige le consommateur vers le site de la banque avec les informations nécessaires à la transaction (montant total, numéro de compte du vendeur…). La banque demande alors au consommateur d'autoriser ce paiement et, si tel est le cas, les fonds sont

immédiatement transférés du compte du consommateur vers celui du marchand, puis la banque redirige le consommateur sur le site web du vendeur.

Toutes ces opérations donnent lieu à une transmission sécurisée et, de plus, le marchand et le consommateur sont identifiés par la banque.

1,6 million de consommateurs finlandais (sur une population totale de 5 millions) ont conclu un tel contrat de banque à distance avec leur banque.

Ce mécanisme est intéressant du point de vue des commerçants, car le paiement précède la livraison du bien vendu et il a un caractère irrévocable. En revanche, le consommateur ne peut récupérer son argent si la livraison n'est pas effectuée. Ce système soulève, en outre, une difficulté pratique : les commerçants sont tenus de disposer d'un compte dans chaque banque pratiquant cette méthode (en Finlande, un compte doit donc être ouvert dans quatre des cinq grandes banques du pays, puisque deux d'entre elles ont néanmoins rendu leurs réseaux interopérables).

B.- Les systèmes privés de compensation

Les systèmes privés de compensation sont des systèmes qui permettent à un mandataire unique le recouvrement de créances consécutif à des transactions réalisées sur une période déterminée. Ces systèmes peuvent être subdivisés en deux classes : le réseau de recouvrement par facture et le réseau de recouvrement en compte.

Le réseau de recouvrement par facture :

Le *kiosque micro*, évolution du *Minitel*, a été lancé sur Internet en avril 1996. Il permet à un abonné de consulter sur son ordinateur des services multimédias. Les services consommés sont payés en fin de mois à réception de la facture.

Le réseau de recouvrement en compte :

Ce système offre aux abonnés le loisir d'ouvrir un compte sur lequel seront enregistrés les achats. Ces derniers seront ensuite réglés par facture. Ainsi, *Wanadoo* propose, depuis juin 1997, un système de facturation à l'acte qui permet à ses abonnés d'acheter de l'information et aux fournisseurs de rémunérer la mise en ligne de leurs services. Le paiement *Wanadoo* permet d'effectuer des achats qui seront portés sur la facture mensuelle *Wanadoo* (les paiements de biens tangibles ne sont pas possibles avec le compte sur facture).

Ces systèmes privés de compensation sont bien adaptés pour payer un marchand que le consommateur contacte régulièrement. Ils semblent, en revanche, peu susceptibles d'être mis en œuvre pour un achat épisodique.

c.- Le numéro de transaction unique

La dernière « mode » en matière de paiement en ligne semble être un dispositif reposant sur le concept du numéro de transaction périssable, en vertu duquel un numéro, choisi au hasard, est utilisé pour une transaction unique à la place du numéro de carte bancaire du client.

La première initiative est due à *American Express*, qui a lancé un projet baptisé « *private payments* ». Tout porteur de carte *American express* est libre de s'inscrire sur le site dédié à cet usage pour bénéficier de ce service gratuit, auquel il peut accéder, par la suite, en communiquant son nom d'usage et un mot de passe. Le numéro périssable qui lui est attribué au moment d'exécuter une transaction en ligne est alors recopié, par ses soins, sur le formulaire d'achat du site marchand et expire dès que la transaction a été réalisée.

Le groupement des cartes bancaires, en France, a également annoncé son intention de développer une « carte virtuelle dynamique », sans donner d'autres précisions.

De nombreux autres dispositifs à numéro périssable sont proposés. Votre Rapporteur a d'ailleurs procédé à l'audition de deux représentants de ces projets (*OSP System et OSmoney*). Le premier cité rejoint le mode de sécurisation faisant intervenir la carte bancaire, puisqu'il peut être mis en œuvre sur un type spécifique de carte comportant un clavier ultra plat et un écran digital (carte déjà développée par la société *Gemplus*). Le second projet, impliquant également l'usage d'un numéro unique pour chaque transaction, se rapproche, en fait, du système notarié en compte, qui a été évoqué précédemment : dans ce cadre, les paiements sont effectués par un intermédiaire de confiance (le « notaire »), dont la fonction est de certifier les termes des transactions et d'authentifier les parties contractantes. Cependant, ces diverses propositions de sécurisation des paiements en ligne supposent la coopération du monde bancaire. Or, ce dernier semble plutôt opter pour une sécurisation bâtie autour de la carte de paiement.

Il est d'ailleurs intéressant de noter que le rapport précité de M. Jean-Michel Yolin, remis au ministre de l'économie, des finances et de l'industrie, indique que « *le plus crédible des concurrents de la carte à puce nous paraît être aujourd'hui l'utilisation directe du téléphone portable, qui intègre une puce comme terminal de paiement électronique* ». Il ajoute : « *évidemment, cette évolution technologique inquiète les banques* ».

IV.- la sécurisation des transactions réalisées par carte de paiement

Les dispositifs présentés précédemment sont des systèmes alternatifs au paiement par carte bancaire, qui, pourtant, apparaît spontanément comme le moyen « naturel » de paiement en ligne. Cela ne signifie pas, d'ailleurs, que les autres procédés doivent être condamnés : en fonction des marchés, des « cultures » en matière de paiement, des besoins, plusieurs mécanismes de sécurisation s'avéreront complémentaires.

En matière de sécurisation des transactions par carte de paiement, la diversité des procédés est également de mise, malgré les tentatives effectuées ces dernières années par le monde bancaire pour imposer la solution *Cyber-COMM*.

A.- des dispositifs dont le niveau de sécurisation est variable

Certaines solutions proposées se révèlent très originales. Ainsi, le bureau d'études et d'ingénierie *elva* développe *VocaliD* qui intègre une touche sensitive permettant l'émission, par effleurement du doigt, d'une séquence sonore d'authentification à validité unique. Au lieu de donner son numéro de carte bancaire, le porteur s'authentifie donc à l'aide d'une séquence sonore émise par la carte.

De façon plus traditionnelle, on distingue généralement les systèmes visant à préserver la confidentialité des données transmises en ligne et ceux mettant en œuvre la lecture de la carte de paiement par un lecteur (connecté ou intégré à l'ordinateur), ce qui évite de faire transiter « en ligne » certaines données.

Le protocole de sécurisation des communications le plus utilisé est le protocole *Secure Socket Layer* (SSL), qui met en œuvre une cryptographie asymétrique, faisant appel à une clef privée (confidentielle) et à une clef publique (connue de tous). Ce protocole de sécurisation des échanges de données a été conçu par *Netscape* et il est installé en standard dans la plupart des navigateurs équipant les ordinateurs.

Deux modèles fondés sur SSL ont été développés : le système SSL intermédié et le système SSL non intermédié. Dans le premier cas, qui représente environ 43% du marché du paiement en ligne par carte bancaire en France (avec notamment *Cybermut* et *Telecommerce*) un intermédiaire non bancaire assure l'interface entre le commerçant, la banque et le client, ce qui évite que le commerçant reçoive le numéro de la carte. Les solutions SSL sans intermédiaire sont les plus utilisées (environ 55% du marché).

SSL permet l'établissement d'un canal de confidentialité pour la transmission du numéro de carte bancaire. Il assure également l'intégrité des messages échangés.

En France, le degré de protection accordé par SSL a pu être élevé grâce à la décision du Gouvernement, en janvier 1999, d'élargir à 128 bits (contre 40 précédemment) le seuil de la cryptologie dont l'utilisation est libre : la longueur des clefs mises en œuvre peut ainsi être équivalente à ce qui est fait notamment aux Etats-Unis.

Il n'en demeure pas moins que la confidentialité de la transmission n'est pas la plus fondamentale des protections, dès lors que les numéros de carte bancaire peuvent être obtenus par d'autres moyens. L'inconvénient majeur de SSL est effectivement de ne pas authentifier les acteurs de la transaction. Dans ces conditions, si SSL est utilisé « en mode natif » (c'est-à-dire sans émission d'un certificat), il est possible pour le consommateur de contester un paiement.

Pour accroître le niveau de sécurisation des transactions et interdire les possibilités de répudiation, différentes initiatives visent à mettre en place un système de lecteur de carte à puce. Là encore, les niveaux de sécurisation sont variables : certains (tels les boîtiers fabriqués par *proton* et diffusés à 200.000 exemplaires en Belgique) se contentent de certifier qu'un code secret a été utilisé ; d'autres lecteurs vont plus loin encore en permettant d'identifier l'utilisateur grâce à la mise en œuvre du protocole de paiement sécurisé *Secure Electronic Transaction* (SET).

Cette sécurisation maximale est celle qui est développée, en France, par *Cyber-COMM*.

B.- les difficultés de la solution cyber-Comm

Trois projets pilotes ont, tout d'abord, été initiés par les banques sur la base unique du logiciel SET :

– le premier, lancé par le consortium *e-COMM*, à la fin de 1996, était soutenu par trois banques (Crédit Lyonnais, BNP et Société générale), Visa et quelques industriels ;

– le second, *C-SET*, conçu par le Groupement des cartes bancaires ;

– le dernier projet, *VSEC*, s'inscrivait dans le cadre d'un projet européen lancé par Visa.

Finalement, une convergence a eu lieu entre ces trois projets, en 1998, sous l'appellation de *Cyber-COMM*.

En pratique, dans le cadre du paiement *Cyber-COMM*, le titulaire de la carte devant un micro-ordinateur relié à un lecteur sécurisé se voit proposer d'introduire sa carte, puis de composer son code secret. La carte à puce contrôle elle-même l'exactitude de ce code et vérifie l'identité numérique de l'utilisateur. L'identification réalisée, les informations sont chiffrées, puis signées par le logiciel du lecteur et transmises à une passerelle de paiement distante, qui authentifie la carte et le lecteur et vérifie l'intégrité des données transmises.

tout le monde s'accorde à dire que ce dispositif offre un niveau de sécurisation maximum.

Fort de ce consensus et de ses certitudes, la communauté bancaire française a longtemps annoncé que *Cyber-COMM* serait LA solution de paiement sécurisée « en ligne ». Ce soutien des banques s'explique d'autant plus que *Cyber-COMM* permettrait de réduire les paiements par chèques (gratuits) et de contrer les autres dispositifs, surtout ceux susceptibles de donner naissance à des monnaies « privées », sur lesquelles les banques n'ont pas de prise.

Pourtant, la diffusion du boîtier *Cyber-COMM* est loin d'avoir répondu aux espérances, alors que, si l'on tient compte des trois projets pilotes, les banques françaises ont déjà investi plusieurs centaines de millions de francs. Actuellement, 20.000 lecteurs seulement sont en fonction (soit un nombre sensiblement inférieur à celui de 500.000 boîtiers que *Cyber-COMM* prévoyait de déployer avant la fin 2001). Encore faut-il ajouter que les lecteurs en fonction sont fort peu utilisés (environ 300 transactions par mois au total, pour des paiements d'un montant moyen de 500 francs). Il est vrai que seulement 25 enseignes commerciales sont équipées pour opérer des transactions par *Cyber-COMM*.

On touche là, d'ailleurs, à l'un des grands problèmes de ce dispositif, qui est l'impérissable question de « l'œuf et de la poule » : les consommateurs ne s'équipent pas parce qu'ils ne trouvent pas de commerces en ligne adaptés au paiement par *Cyber-COMM* ; ces derniers n'investissent pas en ce domaine, car il y a peu de boîtiers diffusés.

D'autres explications, moins métaphysiques, ont pu être avancées pour tenter de comprendre cet insuccès.

On a ainsi fait valoir la complexité d'installation du lecteur sur les ordinateurs personnels (l'idéal serait, bien sûr, un lecteur intégré dans les claviers par les fabricants d'ordinateurs). Or, d'importants efforts ont été réalisés en la matière et, si l'installation n'est pas aussi simple que le branchement d'une prise électrique, elle ne pose pas non plus de problèmes insurmontables, même pour les néophytes.

Une autre difficulté souvent évoquée est celle du coût du lecteur. Alors que des lecteurs moins sécurisés comme ceux de *proton* sont proposés au prix maximum de 200 francs, les lecteurs *Cyber-COMM* sont vendus 400 francs minimum. Toutefois, une protection forte implique une grande puissance de calcul, ce qui a un prix. En outre, ce lecteur peut télécharger les futures adaptations du logiciel et est donc évolutif. Par ailleurs, les enquêtes menées auprès des clients potentiels révèlent que l'argument du coût est peu mis en avant.

En fait, l'obstacle majeur est finalement le protocole SET qui n'a pas pu s'imposer au niveau international.

En 1998, il n'y avait ainsi que 150 banques liées à VISA (dans 39 pays) et

78 banques liées à Mastercard qui prévoyaient de mettre en œuvre ce protocole. De même, il n'y avait que 150 sites commerciaux qui l'acceptaient ().

La situation a peu évolué depuis, ce qui est peu impressionnant pour un standard international ().

Le fait est que les Etats-Unis n'ont guère adhéré à ce protocole : les acteurs du commerce dans ce pays semblent prêts à tolérer un taux de fraude relativement élevé, de la même façon qu'ils ont toléré la fraude sur les cartes à piste magnétique () , dont l'usage est encore largement majoritaire dans ce pays d'ailleurs.

Dans le monde trans-frontières du commerce électronique, les réticences américaines (qui, bien sûr, par un phénomène traditionnel d'imitation, ont conduit la Grande-Bretagne à faire preuve de méfiance) ont provoqué le recul du concept de sécurisation par SET de bout en bout de chaîne de la transaction (avec, en particulier, la mise en place de la norme *3D Secure*, permettant d'opérer avec un commerçant non équipé pour SET, grâce à un intermédiaire).

Face à ces divers revers, *Cyber-comm* a dû s'adapter. Le conseil d'administration du 28 juin dernier a procédé à une réorganisation de l'entreprise et lui a fixé de nouveaux objectifs : « *la structure ne se positionne plus comme la solution française la plus sécurisée à imposer au plan international, mais comme " une des solutions autour de laquelle se bâtiront des systèmes de sécurité forts"* () ».

Chapitre IV :

Le renforcement nécessaire de l'intervention des pouvoirs publics

Les pouvoirs publics français ne peuvent pas se désintéresser des questions touchant à la monnaie et au commerce électroniques et, en particulier, des problèmes de sécurisation. Ces questions sont d'autant plus importantes dans notre pays qu'elles y soulèvent un véritable enjeu industriel. Les entreprises françaises sont, en effet, les *leaders* sur le marché de la carte à puce. Elles subissent actuellement les conséquences du ralentissement de la croissance du secteur de la téléphonie mobile, comme en témoignent les difficultés sociales de *Gemplus*. Il serait dommageable de les fragiliser encore plus en ne prenant pas les mesures nécessaires à une large diffusion du commerce électronique et des moyens de paiement qui lui sont spécifiques.

Fort heureusement le Gouvernement français a conscience de ces enjeux, comme en atteste le mémorandum adressé, en mars 1998, à la Commission européenne et aux Etats membres, prenant position en faveur de la mise en place d'un cadre réglementaire communautaire de nature à stimuler le commerce électronique européen, en répondant aux attentes des entreprises et des consommateurs. En outre, une mission « commerce électronique » a été mise en place au sein du ministère de l'économie, des finances et de l'industrie, dont les principales activités visent, d'une part, à animer des groupes de travail spécialisés regroupant administrations et interlocuteurs externes à l'administration (entreprises, experts…) et, d'autre part, à établir et suivre un tableau de bord des actions relevant des pouvoirs publics. Cette mission, désormais dénommée « mission de l'économie numérique », est présidée par M. Henri Guillaume.

De nombreuses actions ont d'ores et déjà été mises en œuvre, notamment pour adapter le cadre juridique.

Votre Rapporteur considère qu'il convient d'accélérer l'adoption des mesures nécessaires à la constitution de ce cadre légal. Par ailleurs, il lui semble opportun de promouvoir un « modèle européen », s'opposant à la fois aux initiatives trop hexagonales et aux habituelles volontés hégémoniques des Etats-Unis.

I.- Achever rapidement la mise en place d'un cadre juridique adapté

En la matière, il serait souhaitable, d'une part, d'adopter définitivement, au plus vite, les deux projets de loi actuellement soumis au Parlement et, d'autre part, d'envisager de nouvelles initiatives.

a.- adopter au plus vite les projets de loi relatifs À la sÉcuritÉ quotidienne et sur la sociÉtÉ de l'information

Plusieurs textes importants ont déjà été adoptés, que ce soit au niveau communautaire ou au niveau national (ces derniers textes transposant souvent des directives européennes).

Pour s'en tenir à la législation française, on peut citer trois dispositions votées en 2000 :

– la loi n° 2000-642 du 10 juillet 2000 portant réglementation des ventes volontaires de meubles aux enchères publiques, qui a déterminé le cadre juridique applicable aux ventes aux enchères publiques à distance par voie électronique ;

– la loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, qui a précisé le droit applicable aux services de communication en ligne ;

– la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Le décret d'application de cette dernière disposition a été publié, un an plus tard (décret n° 2001-272 du 30 mars 2001). Il détermine les conditions dans lesquelles un procédé de création de signature électronique peut être considéré comme sécurisé. Il est important de signaler que, comme le projet de loi relatif à la sécurité quotidienne donne à la Banque de France la possibilité de rendre publiques les insuffisances des moyens de paiement, le décret précité prévoit que les services du Premier ministre chargés de la sécurité des systèmes d'information doivent assurer la publicité des résultats des contrôles effectués auprès des prestataires de services de certification électronique.

Le projet de loi relatif à la sécurité quotidienne a déjà fait l'objet d'un examen dans l'introduction du présent rapport d'information. On se contentera donc de rappeler qu'il comporte des dispositions essentielles pour la protection des porteurs de carte et que ces dernières sont incontestablement susceptibles de favoriser le développement du commerce électronique. Il est donc regrettable que ce projet de loi n'ait pu être adopté définitivement avant la fin de la session parlementaire, du fait, notamment, de l'interférence provoquée par l'amendement « *rave party* ». Cela retarde d'autant la diffusion de la huitième version du contrat porteur élaboré par le Groupement des cartes bancaires, qui intègre diverses mesures favorables aux consommateurs. Dans ces conditions, il importe que l'achèvement de

la navette entre les deux assemblées du Parlement soit réalisé au plus tôt lors de la prochaine session.

De la même façon, il conviendrait d'inscrire rapidement à l'ordre du jour le projet de loi sur la société de l'information, qui a finalement été déposé par le Gouvernement, le 14 juin dernier, après plusieurs années de concertation et d'élaboration (même s'il est exact que certaines dispositions initialement prévues pour figurer dans le texte sur la société de l'information ont, en fin de compte, été intégrées dans d'autres textes déjà promulgués).

Deux des cinq titres du projet de loi sur la société de l'information intéressent spécialement notre propos :

– le titre III, « Du commerce électronique », transpose la directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques de la société de l'information et notamment du commerce électronique. Il fixe des conditions juridiques claires pour réaliser les échanges électroniques. Il est ainsi prévu que chaque prestataire est soumis à la loi de l'Etat membre dans lequel il est établi. De même, un principe d'identification de toute personne ou entreprise exerçant une activité commerciale *via* des services de communication en ligne est institué. Par ailleurs, la valeur juridique du contrat électronique est reconnue ;

– le titre V, « De la sécurité dans la société de l'information », renforce les moyens dont disposent la police et la justice pour lutter contre la cybercriminalité et procède à la mise à jour de la réglementation touchant à la cryptologie. Il met ainsi en œuvre la libéralisation de l'utilisation de la cryptologie annoncée lors du comité interministériel du 19 janvier 1999, tout en renforçant les moyens de lutte contre l'usage de la cryptologie à des fins délictueuses.

Ces mesures sont indispensables pour créer un environnement sécurisé. Les pouvoirs publics peuvent, néanmoins, proposer d'autres dispositions relevant du champ de leurs compétences.

b.- prendre de nouvelles initiatives

Ces initiatives pourraient être d'ordre législatif et pratique.

1.- Impliquer les commerçants dans la sécurisation

Il ne sert à rien de déployer d'importants efforts au niveau juridique et au niveau technique pour sécuriser les transactions, si tous les commerçants ne prennent pas clairement conscience des enjeux.

Les commerçants doivent donc être impliqués dans la politique de sécurisation, ce qui n'est pas forcément le cas aujourd'hui.

On sait parfaitement, par exemple, que des opérateurs de téléphonie mobile privilégient volontairement la croissance de leurs chiffres d'affaires à la lutte contre

la fraude, ce qui explique les taux de fraude stupéfiants qu'ils ont pu enregistrer en 2000 et qui ont fortement contribué à la fragilisation de la confiance du grand public dans les cartes bancaires.

De même, de nouveaux entrants dans le monde de la vente à distance ne prennent pas toujours les précautions minimales, alors que « *les sites marchands qui utilisent des bons de livraison découragent 90% des fraudeurs* », aux dires du directeur général du courtier en assurance spécialisé dans ce secteur, *Fia Net*.

Enfin, comme l'observe le rapport précité de M. Jean-Michel Yolin, « *si personne ne rapporte le cas de vols, pendant leur transmission, de numéros de cartes protégées par le cryptage standard (SSL), on ne compte plus le nombre de magasins ou de banques dévalisés de leurs précieux fichiers de cartes de crédit* ».

Des mesures devraient donc être proposées pour sensibiliser les entreprises à la sécurité, voire les pénaliser.

Ainsi, pourrait être envisagée une « labélisation » (prenant la forme d'un logo spécifique) des sites présentant des garanties suffisantes. Cette « labélisation » serait effectuée par une autorité publique, qui pourrait d'ailleurs être une émanation de l'Observatoire de la sécurité des cartes de paiement prévu par le projet de loi relatif à la sécurité quotidienne.

Une autre action de sensibilisation pourrait viser à impliquer les compagnies d'assurance pour qu'elles réduisent les primes versées par les entreprises investissant dans la sécurisation.

Enfin, dans l'hypothèse où des porteurs de carte seraient victimes de fraudes, à la suite du vol de leurs coordonnées dans des bases de données insuffisamment protégées, il devrait être possible de mettre en cause la responsabilité des commerçants imprudents.

2.- Etudier la mise en place d'une carte de citoyen électronique

L'Etat donne déjà l'exemple en ayant procédé à la dématérialisation des procédures administratives (en particulier la télé-déclaration et le télé-règlement de la TVA), ainsi qu'à celle des marchés publics. Ces initiatives peuvent inciter les entreprises à entrer dans les circuits des échanges électroniques.

L'Etat aurait également la faculté de familiariser les particuliers avec le concept de signature électronique, en étudiant la faisabilité technique et juridique d'une distribution, à terme, d'une carte d'identité à puce, permettant également d'authentifier une transaction en ligne. De telles cartes sont déjà en circulation dans certains pays (Finlande, Venezuela…).

ii.- promouvoir un « modÈle europÉen »

« *Les responsables politiques ne doivent pas essayer d'imposer des*

standards ». Cette affirmation formulée par le rapport précité de l'Observatoire européen ESTO est partagée par l'ensemble des intervenants. Ainsi, M. Yves Randoux, administrateur du Groupement des cartes bancaires, écrit-il que « *le marché, dans son pragmatisme habituel, tranchera entre les meilleurs outils* » ().

Cela ne signifie pas, pour autant, que les pouvoirs publics doivent « laisser faire ». Il est d'ailleurs significatif que, dans le même article, M. Yves Randoux déclare : « *nous inviterons les responsables européens à prendre conscience de la formidable opportunité qui s'offre à eux d'assurer massivement le succès de cette opération en accompagnant, à travers le cadre institutionnel existant, le protocole proposé par* Cyber-comm ».

Les enjeux monétaires économiques, industriels imposent effectivement que « *les pouvoirs publics ne peuvent pas ne pas agir* » (). L'Observatoire européen ESTO note d'ailleurs que s'ils ne peuvent imposer des standards, les responsables politiques ont néanmoins la possibilité de favoriser leur émergence « *en les utilisant, en soutenant des projets pilotes et en finançant des recherches* ».

Votre Rapporteur estime que l'action des pouvoirs publics, en la matière, doit poursuivre un double objectif :

– favoriser l'apparition de dispositifs interopérables au niveau européen, et d'un niveau élevé de sécurisation, d'une part ;

– préserver les compétences que l'Europe a acquises en ce domaine, d'autre part.

A.- Favoriser l'apparition de dispositifs interopÉrables et sÉcurisÉs

Les autorités étatiques et européennes n'ont pas la capacité d'imposer, par exemple, l'usage du protocole *cyber-COMM*. La réglementation du droit de la concurrence les en empêcherait. Il n'est donc pas possible d'envisager la prise en charge par l'Etat d'une diffusion massive et gratuite du boîtier auprès des internautes, sur le modèle de ce qui a été réalisé pour le *Minitel*.

S'il n'est pas possible, ni même souhaitable, de soutenir particulièrement un moyen spécifique de paiement (ne serait-ce, d'ailleurs, que parce que les utilisateurs sont demandeurs de plusieurs dispositifs, qui coexisteront pour satisfaire des besoins différents selon les transactions et les cultures nationales en matière de paiement), il est, en revanche, indispensable d'unifier les infrastructures.

On ne peut qu'être frappé par la similitude des schémas évolutifs des projets de porte-monnaie électroniques et de lecteurs sécurisés pour les transactions sur Internet. Dans les deux cas, plusieurs projets isolés ont tenté de développer leur standard spécifique, sans tenir compte de ce qui se faisait par ailleurs. Dans les deux cas, ces projets ont fini par se regrouper sous la houlette du Groupement des cartes bancaires, qui travaille à assurer la cohérence et la pérennité de ces dispositifs ; action qui mérite d'être saluée et soutenue.

Cette situation n'est pas spécifique à la France. L'Europe connaît une « balkanisation » des porte-monnaie électroniques, puisque les produits développés sont totalement incompatibles entre eux et limités à un usage réservé à leur propre pays, ce qui est proprement absurde à la veille du passage à l'euro.

Il en découle, bien sûr, des gaspillages de temps et d'argent, qui ne peuvent que favoriser les concurrents de l'Europe.

« *L'expérience a prouvé que des systèmes fermés privatifs ne pouvaient pas réussir à se développer suffisamment. Seuls, des systèmes techniquement standardisés, et assurant l'interbancarité peuvent arriver à s'imposer et atteindre une taille critique* » ().

Il convient donc d'édicter des normes communes au niveau européen, normes que les différents fabricants devront respecter. Le GSM a montré qu'il est possible de faire naître en Europe une norme commerciale internationale.

Des initiatives sont d'ores et déjà en cours.

Le groupe CEPS (*Common Electronic Purse Spécifications*) s'est donné pour ambition de définir les standards du porte-monnaie électronique.

De même, en ce qui concerne, les lecteurs de cartes à puce sécurisés, un processus de standardisation est en cours, sous l'égide de la Commission européenne. Il s'agit du projet *finread* (*Financial transactional IC card Reader*).

Les pouvoirs publics ne doivent pas se contenter d'initier des normes communes. Il importe de veiller également à ce que ces normes aient un niveau de sécurisation suffisamment élevé, ce qui implique des révisions régulières pour maintenir les fraudeurs à bonne distance.

Ainsi, le protocole SET ne doit-il pas être considéré comme définitivement obsolète, alors qu'il est unanimement reconnu comme le plus sûr.

Par ailleurs, votre Rapporteur estime qu'il serait opportun de favoriser dès à présent, les recherches en matière de biométrie. Cette technologie fait déjà l'objet d'avancées significatives, même si, là encore, des problèmes de standardisation existent. La société *Gemplus* a ainsi développé particulièrement la reconnaissance par empreintes digitale et par la voix. De même, pour éviter des problèmes de fiabilité, *Proton* étudie un système combinant la frappe d'un code secret, la reconnaissance de la voix et celle du visage. Les industriels ont tendance à ne voir dans la biométrie qu'une technologie qui s'imposera à long terme, alors qu'elle est susceptible de sécuriser très fortement le commerce électronique. Les pouvoirs publics ont donc ici un rôle à jouer pour favoriser les recherches ou imposer que les nouveaux terminaux soient compatibles, dans un proche avenir, avec un support biométrique.

B.- préserver l'acquis européen

La carte à puce est une création française qui a su s'imposer au niveau mondial. Pendant longtemps, les Etats-Unis ont observé cette technologie avec un brin de condescendance, n'en comprenant pas l'intérêt. Les cartes à piste magnétique semblaient répondre à leurs besoins, d'autant que leur système de paiement diffère sensiblement de celui que nous connaissons en France : les cartes sont essentiellement des cartes de crédit, ce qui implique que les consommateurs reçoivent un relevé avant d'être débités et qu'ils ont une large capacité de répudiation. En outre, les transactions sont effectuées « en ligne », avec l'intervention de questions personnalisées facilitant l'authentification du porteur.

Ce dispositif n'a pas empêché, néanmoins, le développement de la fraude aux Etats-Unis et le regard porté sur la carte à puce a changé, comme en témoigne le lancement récent de la carte « *Blue* » d'*American express* ().

Il ne faudrait pas, cependant, qu'après avoir négligé cette technologie, les Etats-Unis en prennent le contrôle. Pourtant, une évolution en ce sens semble se dessiner.

La nouvelle norme internationale de la carte à puce – la norme EMV (Europay, Mastercard, Visa) – a, comme son nom le laisse transparaître, largement été définie sous l'égide d'organismes américains.

Il est également inquiétant de voir qu'un fleuron français de ce secteur, la société *Gemplus*, pourrait voir son centre décisionnel transféré aux Etats-Unis. Les mouvements sociaux récents ayant affecté cette entreprise ont ainsi mis en évidence que, depuis que le fonds d'investisseurs *Texas Pacific Group* a acquis 30% du capital et qu'un directeur général américain a été nommé, il est sérieusement envisagé de redéployer les activités sur le continent américain, ce qui pourrait aboutir au transfert de nombreux brevets.

Dans un autre domaine, celui des autorités de certification des signatures électroniques, il importe de signaler que toutes ces organisations sont elles-mêmes certifiées à un niveau hiérarchique supérieur. Or, aujourd'hui celui-ci est essentiellement américain, avec en particulier un organisme nommé *Identrus* (même si l'on voit apparaître d'autres initiatives comme *Certinomis* de La Poste associée à Sagem). « *Sans prêter à ceux-ci le moins du monde la volonté de privilégier les entreprises anglo-saxonnes, on ne peut s'empêcher de penser que très naturellement ils favoriseront les entreprises qui leur sont culturellement et économiquement proches et l'on peut s'interroger sur l'opportunité de prendre des initiatives dans ce domaine au niveau national, ou plus vraisemblablement européen* » ().

Votre rapporteur ne peut qu'approuver cette dernière suggestion et, de façon plus générale, inciter les pouvoirs publics à promouvoir un véritable modèle européen de sécurisation, tirant pleinement partie des connaissances et des expériences acquises. Cela semble être le seul moyen de préserver la confiance des consommateurs, en maintenant le niveau de sécurisation à une longueur d'avance des compétences des fraudeurs.

examen en commission

La Commission a examiné le présent rapport d'information au cours de sa séance du 11 juillet 2001.

Votre Rapporteur a rappelé qu'une bonne partie du sujet avait déjà été traitée dans le cadre du rapport pour avis sur le projet de loi relatif à la sécurité quotidienne. A cette occasion, plusieurs propositions ont pu connaître une traduction législative, au travers notamment de l'augmentation du rôle de la Banque de France en matière de sécurité des moyens de paiement scripturaux, de l'adaptation du dispositif pénal et de l'approfondissement des garanties des titulaires de cartes bancaires. En outre, il convient de signaler la création de l'Observatoire de la sécurité des cartes de paiement, qui devrait comporter, en son sein, une cellule de veille technologique, associant les diverses administrations concernées par la lutte contre la fraude, ce qui devrait permettre d'assurer une meilleure coordination de leurs actions.

Il a noté que le rapport présenté aujourd'hui était davantage orienté sur l'évolution et la diversification des moyens de paiement ainsi que sur la sécurisation des transactions dans le domaine du commerce électronique. La perspective est différente et s'attache davantage à l'enjeu industriel de ces questions, dans la mesure où les entreprises françaises restent leader sur le marché de la carte à puce. Si les mesures nécessaires en matière de sécurisation des transactions ne sont pas prises, on peut craindre que cette avance ne s'érode. La France a, à cet égard, transmis, en 1998, un mémorandum à la Commission européenne, en vue de la mise en œuvre d'un cadre réglementaire visant à assurer la promotion d'un modèle européen de sécurité des cartes bancaires. Il convient, en effet, de ne pas s'enfermer dans des initiatives hexagonales et de faire face aux tentatives hégémoniques des Etats-Unis, qui souhaitent combler leur retard. La question de la délocalisation aux Etats-Unis des centres de décision d'une entreprise comme *Gemplus* est, à cet égard, très significative.

Il a déploré que le projet de loi relatif à la sécurité quotidienne n'ait pu être adopté définitivement. Par ailleurs, le projet de loi sur la société de l'information aborde également la question de la sécurité des moyens de paiement, notamment au travers de son titre III, traitant du commerce électronique et de son titre V, portant sur la sécurité dans la société de l'information, lequel renforce les moyens de lutte de la justice et de la police contre la cybercriminalité et procède à une adaptation des mesures relatives à la cryptologie.

Faisant part des propositions contenues dans le rapport, il a indiqué qu'il conviendrait d'associer davantage les commerçants aux procédures de sécurisation. Cette observation vaut notamment pour les opérateurs de téléphonie mobile qui, à l'exception de *France Télécom*, ont privilégié une surenchère commerciale et la croissance de leur chiffre d'affaires au détriment de l'amélioration de la sécurité. Le taux de fraude d'un des opérateurs a d'ailleurs dépassé les 10%.

Il convient, afin de ne pas fragiliser la confiance des consommateurs envers la carte de paiement, que les nouveaux entrants dans le marché de la vente à distance prennent toutes les mesures de sécurité nécessaires, s'inspirant en cela des procédures mises en œuvre par les entreprises habituées à travailler depuis longtemps dans le domaine de la vente par correspondance.

Afin de sensibiliser les entreprises à l'importance d'une telle sécurisation, il serait possible d'imaginer une labélisation par une autorité publique, permettant de reconnaître les sites présentant un niveau de garantie suffisant. Il conviendrait, en outre, d'inciter les compagnies d'assurance à diminuer les primes demandées aux entreprises investissant dans les dispositifs de sécurisation. Par ailleurs, la mise en cause de la responsabilité des commerçants imprévoyants, se faisant piller leurs bases de données trop peu protégées, pourrait être envisagée.

D'un point de vue plus général, il faut favoriser la mise en œuvre de dispositifs interopérables au niveau européen, afin de préserver l'avance de l'Union européenne en la matière. Actuellement, il est inenvisageable d'imposer tel ou tel moyen de sécurisation, qu'il s'agisse du protocole *Cyber-COMM* ou du système belge *Proton*. Inversement, il convient d'aller vers un cadre réglementaire favorisant l'interopérabilité. En effet, il est absurde, par exemple, que les divers dispositifs de porte-monnaie électroniques ne soient pas compatibles. La norme GSM en matière de téléphonie mobile a bien montré qu'une telle interopérabilité était possible, à condition de s'appuyer sur une véritable volonté politique. Des initiatives dans ce sens sont d'ailleurs en cours, s'agissant du porte-monnaie électronique et des lecteurs sécurisés. Des normes communes ne suffisent pas ; les pouvoirs publics devront aussi veiller à maintenir régulièrement un niveau de sécurisation suffisant.

Il faut aller plus loin dans le développement des dispositifs de sécurisation et marquer de l'intérêt, non seulement pour des systèmes comme *Cyber-COMM*, mais aussi pour des technologies encore plus innovantes comme la biométrie. Déjà utilisée par les militaires, celle-ci nécessite des recherches supplémentaires pour améliorer la fiabilité de la reconnaissance des individus et réduire les marges d'erreur sur l'analyse des empreintes digitales ou de la voix.

En définitive, il est incontestable que les moyens existent de sécuriser fortement le commerce électronique, qui pourra de ce fait se développer et s'imposer.

Dans le rapport qu'il a remis récemment au Secrétaire d'Etat à l'industrie, M. Jean-Michel Yolin estime à juste titre que, sans prétendre imposer une hégémonie sur un secteur en plein développement, les Etats-Unis devraient favoriser les entreprises qui leur sont proches, aux plans culturel et économique. Il est donc nécessaire de prendre des initiatives visant à promouvoir un « modèle européen de sécurisation », afin, d'une part, de préserver la confiance et l'intérêt des consommateurs et, d'autre part, d'assurer la pérennité d'un secteur industriel qui pâtit des difficultés rencontrées, par ailleurs, dans le domaine de la téléphonie mobile. Le commerce électronique est, pour sa part, un « créneau » porteur spécifique qui justifie que des efforts particuliers soient entrepris en sa faveur. De

plus, on peut imaginer une extension des technologies mises en œuvre à d'autres domaines, comme par exemple le développement des téléprocédures. Sans vouloir faire preuve d'un excès d'optimisme, le temps n'est peut-être pas loin où l'on pourra disposer d'une carte électronique « citoyenne », servant à la fois de carte d'identité, de porte-monnaie électronique et de carte de paiement.

M. Gilbert Gantier, Président, a souligné que, si l'usage des cartes de paiement pose peu de problèmes de fraude, en France, grâce à la généralisation de la carte à puce, il n'en va certainement pas de même à l'étranger, où l'on voit encore beaucoup de « fers à repasser ».

Votre Rapporteur a confirmé la justesse de cette analyse, mais a rappelé qu'en France, les banques avaient parfois tardé à mettre en œuvre leurs engagements en matière de sécurité des moyens électroniques de paiement. Par exemple, il est de notoriété publique que certains réseaux bancaires ont été longs à s'équiper de distributeurs de billets capables de lire la carte à puce. De tels distributeurs et des terminaux de paiement commencent à apparaître aux Etats-Unis, qui ont découvert beaucoup plus récemment les vertus de la carte à puce. Mais la bataille industrielle n'est pas gagnée : on doit se souvenir que les Etats-Unis ont, semble-t-il, caressé un temps le projet de modifier l'emplacement de la puce sur la carte, ce qui aurait disqualifié *de facto* le système français.

La Commission a ensuite *autorisé,* en application de l'article 145 du Règlement, la publication du rapport d'information.

ANNEXES

ANNEXE I

PRINCIPALES PROPOSITIONS CONTENUES DANS LE PRÉSENT RAPPORT D'INFORMATION

Ces propositions et suggestions s'adressent aussi bien au Gouvernement qu'aux autorités européennes.

– au Gouvernement :

Il lui appartient, tout d'abord, de veiller à inscrire rapidement à l'ordre du jour de la prochaine session parlementaire le projet de loi relatif à la sécurité quotidienne (dont une nouvelle lecture doit avoir lieu au Sénat avant, le cas échéant, une adoption définitive à l'Assemblée nationale) et le projet de loi sur la société de l'information.

Ce dernier texte pourrait d'ailleurs être amendé pour prévoir des sanctions à l'égard des sites marchands « en ligne » dont les bases de données ne sont pas suffisamment sécurisées. L'objectif poursuivi par cette dernière mesure pourrait également être atteint grâce à des actions incitatives : labélisation par une autorité publique des sites sécurisés et réduction des primes d'assurance des entreprises investissant dans cette sécurisation.

Par ailleurs, sous réserve d'une appréciation juridique plus poussée, le Gouvernement pourrait étudier la création d'une carte d'identité à puce, permettant de réaliser des signatures électroniques.

– aux autorités européennes :

A ce niveau où le Gouvernement français a également un rôle important à jouer, il importe de promouvoir un « modèle européen » des moyens de paiement électronique.

Cela implique, tout d'abord, de soutenir les actions visant à développer l'interopérabilité des divers dispositifs.

Cela conduit, ensuite, à imposer des normes minimales de sécurisation et à veiller sur leur caractère évolutif. En la matière, il importe d'attirer l'attention sur les systèmes mettant en œuvre le protocole de sécurisation SET et de prévoir, dès à présent, une évolution vers des techniques de biométrie.

Cela suppose, enfin, de défendre les acquis de l'industrie européenne de la

carte à puce, face aux convoitises des américains qui n'ont perçu que très récemment l'intérêt majeur de cette technologie.

ANNEXE II

sigles utilises

B2B	:	*Business to business*
B2C	:	*Business to consumer*
EDI	:	Echanges de données informatisées
EMV	:	*Europay, Mastercard, Visa*
ESTO	:	*European science and technology observatory*
PKI	:	*Public key infrastructure*
PME	:	Porte-monnaie électronique
SET	:	*Secure electronic transaction*
SSC	:	*Secure socket layer*
TPE	:	Terminal de paiement électronique

ANNEXE III

liste des personnes entendues

I. ENTRETIENS

– M. François PATRIAT : Secrétaire d'Etat chargé des petites et moyennes entreprises, du commerce, de l'artisanat et de la consommation.

– **Ministère de l'économie des finances et de l'industrie** : Mme Marie-Anne BARBAT-LAYANI, chef du bureau « Etablissements de crédit et entreprises d'investissement » de la direction du Trésor.

– **Ministère de la justice** : M. Philippe LAGAUCHE, chef du bureau de la législation en matière économique et financière ; Mme Nadège MAHE, magistrat.

– **Ministère de l'intérieur** : Mme Catherine CHAMBON, adjointe à l'Office central de répression du faux monnayage.

– **Banque de France** : M. Didier BRUNEEL, directeur général des opérations ; M. Yvon LUCAS, directeur des systèmes de paiement.

– **Groupement des cartes bancaires** : M. Michel RENAULT, président du conseil de direction ; M. Yves RANDOUX, administrateur.

– **Fédération des banques françaises (FBF)** : M. Philippe GIRAUD-SAUVEUR, directeur des systèmes de paiement et de l'organisation ; M. Pierre SIMON, directeur général de l'association française des établissements de crédit et des entreprises d'investissement ; M. Michel GOUDARD, directeur de la chambre syndicale des banques populaires.

– **Fédération du commerce de France** : M. Beaudoin MONNOYEUR, président ; M. Jean-Marc MOSCONI, délégué général de Mercatel.

– **Fédération des entreprises de vente à distance (Fevad)** : M. Bernard SIOUFFI, délégué général.

– **Cegetel** : M. Alain ROCHETTE de LEMPDES, directeur gestion clients ; M. Pierre-Luc REFALO, directeur confiance et sécurité des technologies de l'information.

– **Gemplus** : M. Olivier TREBUCQ, direction plan et stratégie ; M. Rémy MEDEVIELLE ; M. Michel LEDUC, *smart object marketing director*.

– **Cyber-COMM** : M. Michel RENAULT, président ; M. Claude MEGGLE, directeur de la sécurité.

– **Association consommation, logement et cadre de vie (CLCV)** : Mme Reine-claude MADER, secrétaire générale.

– **Association française des usagers des banques (AFUB)** : M. Serge MAITRE, secrétaire général.

– **Association Force ouvrière consommateurs (AFOC)** : M. Eric AVRIL, secrétaire général ; M. Charles REGUARDATI.

– M. Laurent PELE : responsable du site internet « parodie.com », et secrétaire de l'association des victimes de la fraude à la carte bancaire.

– M. Serge HUMPICH.

– M. Roland MORENO, président d'Innovation.

– M. Georges LIBERMAN, président de Xiring.

– M. Ghislan MORET de ROCHEPRISE : OSP System.

– M. David IFERGAN : OSmoney.

– M. Jacques STERN : directeur du département de l'informatique de l'Ecole normale supérieure (Ulm).

II. DÉPLACEMENTS

– **Gémenos** : site de la société Gemplus.

– **Bruxelles** :

• Commission européenne (direction générale du marché intérieur) : M. Jean-Claude THEBAULT ; M. Jean ALLIX ; Mme Catherine GONDELMANN-BREDIN.

• Proton World : M. Armand LEEKENS, *managing director* ; Mme Dominique HAUTAIN, *executive vice-président*.

• Eurosmart : Mme GRAS.

3229. - Rapport d'information (art. 145) de M. Jean-Pierre Brard sur la sécurité des cartes bancaires (commission des finances)

(

1) *Electronic payment systems observatory (EPSO), dont le siège est à Séville.*
(2) La Tribune*, 25 avril 2001, p. 28.*
(3) *Etude remise en mars 2001 et réalisée par un consortium de dix partenaires européens.*
(4) *«* Study on electronic payment systems *» for the committee on economic and monetary affairs and industrial policy of the european parliament, mai 1999, p. 27.*
(5) *Un contrat type spécifique à la vente à distance impose des obligations supplémentaires aux commerçants concernés.*
(6) *Lors de son audition par votre Rapporteur, le 6 juin dernier, le Conseil du commerce de France a considéré qu'environ 500.000 TPE étaient en mesure d'éditer des tickets conformes aux recommandations édictées par la charte du 22 février 2001.*
(7) *Lors de l'audition précitée, le Conseil du commerce de France a indiqué qu'actuellement 350.000 TPE sont déjà adaptés à cette nouvelle norme.*
(8) *Ces derniers ne concernant pas, en pratique, les consommateurs, le présent rapport ne les étudiera pas de façon spécifique.*
(9) *David Bounie et Livio Vaninetti, «* Les implications monétaires du développement des systèmes de paiement électronique *», Revue économique, 2001.*
(10) *Pierre Gazé, «* Le porte-monnaie électronique : quelques enjeux stratégiques pour l'industrie bancaire *», Revue d'économie financière n° 53, 1999.*
(11) *Rapport de la mission conduite par M. Jean-Michel Yolin, «* Internet et entreprise, mirage ou opportunité ? *», mise à jour 2001.*
(12) *«* Electronic payment systems in european countries *», septembre 1999.*
(13) *Francis Lorentz, synthèse du rapport «* La nouvelle donne du commerce électronique ; réalisations 1998 et perspectives *».*
(14) *David Bounie et Livio Vaninetti, article précité.*
(15) *Eric Brousseau, «* Commerce électronique : ce que disent les chiffres et ce qu'il faudrait savoir *», Economie et statistique, n° 339-340, 2000.*
(16) *Ces chiffres concernent 1998.*
(17) *Rapport «* La nouvelle donne du commerce électronique, réalisations 1998 et perspectives *» ; rapport du groupe de travail n° 1.*
(18) *Revue de la concurrence et de la consommation, mars-avril 2000, p. 17.*
(19) *Rapport de M. Jean-Michel Yolin, précité.*
(20) *Yves Randoux, «* La sécurisation du paiement sur les réseaux ouverts *», Revue d'économie financière, n° 53, 1999.*
(21) *«* Le commerce de détail s'initie à la vente sur Internet *», INSEE Première n° 771, avril 2001.*
(22) *Les plus pointilleuses des typologies distinguent également le C2C (*consumer to consumer*), le C2B (* consumer to business*), le G2B (*government to business*), etc…*
(23) *Rapport «* La nouvelle donne du commerce électronique : réalisations 1998 et perspective *» ; rapport du groupe de travail n°14.*
(24) *Le protocole SET est également fortement soutenu en Finlande par la banque Luottokunta, mais, fin décembre 1998, il n'y avait que 10.000 logiciels « wallet » qui avaient été téléchargés.*
(25) *On peut observer que, de la même façon, en France, les grandes enseignes de la vente à distance affirment ne pas avoir besoin de* Cyber-comm*, puisque leurs propres dispositions pour combattre la fraude – notamment le suivi des habitudes de leurs clients – seraient suffisantes. De plus, elles pensent que* Cyber-comm *pourraient faciliter l'accès de nouveaux entrants à la vente à distance, ce qui va à l'encontre de leurs intérêts.*
(26) Les Echos*, 3 juillet 2001, p. 23.*

(27) *«* La sécurisation du paiement sur les réseaux ouverts *», article précité, p. 59.*
(28) *Rapport précité de M. Jean-Michel Yolin.*
(29) *Rapport précité* « La nouvelle donne du commerce électronique : réalisations 1998 et perspectives » *; rapport du groupe de travail n° 14.*
(30) *Sur ce point, voir le rapport pour avis sur le projet de loi relatif à la sécurité quotidienne (n° 2992), p. 53.*
(31) *Rapport précité de M. Jean-Michel Yolin.*