CYBERCRIMINALITÉ ET CARTES BANCAIRES À PUCE : UN ENJEU STRATÉGIQUE POUR LA PREUVE DANS LES TRANSACTIONS ÉLECTRONIQUES

YVES RANDOUX*

La lutte incessante, à laquelle se livrent les spécialistes de la sécurité et les faussaires aux connaissances scientifiques plus ou moins étendues, se déroule depuis peu dans le domaine de la technologie des cartes à puce. La carte émise par les grands réseaux mondiaux (Visa, MasterCard, Amex, JCB...) repose sur une technologie obsolète : la piste. Copiée, recopiée, dupliquée, clonée aux hasards des fraudeurs et parfois avec l'aide de quelques rares commerçants complices, cette carte à piste est largement dépassée avec des taux de fraude alarmistes mais auxquels le public, en France, accorde peu d'importance car il dispose d'une carte à puce, sur laquelle les banques « CB » ont investi lourdement, dans les années 1990, avec un succès public renouvelé année après année.

Depuis deux ans, hasard ou manipulation (?), le système « CB » fait l'objet d'attaques récurrentes, largement sans fondement, mais relayées volontiers par les médias. Qu'y a-t-il exactement derrière cette agitation ? A quel enjeu sécuritaire le système « CB » doit-il faire face ? Les réflexions et analyses sur ces deux thèmes sont effectivement essentielles car l'avenir du système « CB » repose sur le haut niveau de sécurité qu'il est capable d'offrir, de maintenir et surtout d'anticiper face aux attaques dont il est désormais l'objet.

L'IRRUPTION DE LA CYBERCRIMINALITÉ DANS UN UNIVERS CLASSIQUE

La fraude est inhérente à tout système de paiement. Une brève typologie des malversations les plus fréquentes, alliée à une réflexion sur les motivations des cybercriminels, illustre les méfaits de la délinquance financière dans tous les systèmes économiques qu'elle gangrène.

La typologie des fraudes, recensées par le système « CB » depuis son existence, n'a pas varié : quatre motifs sont essentiellement utilisés pour retracer les malversations à l'encontre du système : la perte, le vol, la contrefaçon ou la non-réception de la carte par le destinataire.

Cette liste restreinte n'est plus, à l'évidence, susceptible de retracer la diversité des fraudes récentes, plus spécifiquement celles liées à l'usage du numéro de la carte à puce.

Pour bien cerner le phénomène émergent de la cybercriminalité, il faut distinguer les actions frauduleuses effectuées avec

* Administrateur du Groupement des cartes bancaires « CB ».

ou sans l'utilisation de cartes, des divers mécanismes d'incitations à la fraude que recèle le Web.

Fraude avec présence de la carte

La fraude avec présence de la carte : c'est la technique appelée *white plastic* ou *skimming*. Le fraudeur capture, par l'intermédiaire d'un lecteur additionnel connecté à un PC par exemple, les données de la piste magnétique, et réussit, par ruse, à s'emparer du numéro de code confidentiel du porteur. Fort de ces deux données, il reporte sur une carte blanche, dotée d'une piste magnétique vierge, les informations capturées préalablement (d'où le nom de *white plastic*, car ce sont des supports sans graphismes ne coûtant que quelques francs). La cible d'utilisation préférée du faussaire dans ce cas est le distributeur automatique de billets (DAB).

Une seconde technique existe depuis plusieurs années ; en revanche, sa mise en œuvre est récente : la Yescard. Une Yescard est une carte à puce dont le fraudeur a réussi à fabriquer ou à copier la valeur d'authentification statique[1] fournie par la carte à puce et dont le programme de dialogue, avec le terminal, a été modifié notamment pour répondre « oui » à la composition de n'importe quel code confidentiel.

Cette manipulation est possible à partir notamment de la connaissance des spécifications du programme du terminal et des améliorations apportées de façon cumulative dans divers forums de discussion sur Internet, à chaque fois qu'une difficulté surgissait. Les données ainsi « refabriquées » sont insérées dans une carte à puce vierge à l'aide d'outils que l'on peut se procurer dans les magasins spécialisés en électronique pour quelques centaines de francs.

Aujourd'hui, le système « CB » est visé, mais demain ce peut être la carte Sésam Vitale, la carte des décodeurs TV, les badges d'accès à une entreprise…

Ce type de fraude est « facile » pour un « professionnel » lorsque l'algorithme de l'une des clés de protection du système est cassé. Dès lors que les clés ont été modifiées ou que d'autres parades ont été ponctuellement insérées dans les terminaux, la Yescard ne fonctionne plus. Elle ne peut fonctionner en outre que sur des automates, c'est-à-dire pour des achats de faible montant et, en tout état de cause, pour des montants limités en dessous du seuil de demande d'autorisation du commerçant. Structurellement, elle ne peut, comme dans le cas de *white plastic*, être utilisée sur un distributeur automatique de billets.

Fraude sans présence de la carte

La fraude sans présence de la carte se situe essentiellement dans la vente à distance et notamment lors d'un paiement chez un cybercommerçant. De quoi s'agit-il ? Un commerçant propose des produits ou services sur Internet et accepte le paiement par carte bancaire.

L'internaute saisit sur son écran, au moment de payer, les seize chiffres du numéro de la carte et la date de validité. Mais, si ces deux éléments ont été volés (par capture des données sur le Web par exemple), il est facile de les saisir sur écran, et les contrôles informatiques seront dupés. Bien entendu, le fraudeur donne une fausse adresse de livraison et sera probablement lui-même présent lors de la récupération du bien illicitement commandé.

Ce cas reste relativement fréquent sur Internet même si la plupart des entreprises ont déployé des dispositifs sophistiqués pour détecter et réduire ce risque.

Une illustration concrète de cette fraude sans la présence de la carte s'est déroulée l'an dernier dans le secteur des « services immatériels à consommation immédiate » : le rechargement des téléphones mobiles. L'origine de la fraude n'est pas un détournement de la technolo-

gie. C'est plus prosaïquement une faille dans l'organisation administrative des opérateurs téléphoniques. Ainsi, la police a eu, par exemple, l'occasion d'expliquer que, dans les cours de récréation, des jeunes de 12-15 ans, après avoir copié le numéro de la carte à puce de leurs parents, le « revendaient » pour se faire de l'argent de poche ! Ce numéro était ensuite utilisé par un tiers pour recharger son téléphone mobile auprès d'un centre d'appel, à l'insu bien entendu du titulaire de la carte, qui se voyait par exemple débité de deux ou trois rechargements mensuels alors que, bien souvent, il ne possédait même pas de téléphone mobile ! Cette délinquance astucieuse a été présentée, l'an dernier, comme une défaillance de la carte à puce alors que, précisément, elle n'était pas utilisée car non présente physiquement lors de la transaction à distance ! La fraude a porté néanmoins sur plusieurs dizaines de millions de francs.

Les sites Web dédiés au « carding »

Les sites Web dédiés au *carding* représentent une forme récente de cybercriminalité. De quoi s'agit-il ? Les numéros des cartes bancaires répondent à une logique d'émission décrite dans la norme ISO 78-12, libre d'accès comme toute norme ISO. Globalement, la norme découpe le numéro de la carte en deux zones : l'une dédiée au numéro de la banque, c'est le BIN (*Bank Identification Number*) et l'autre attribuée au porteur de la carte, dont elle constitue l'identifiant pointant sur son compte bancaire. L'ensemble est protégé contre les erreurs de recopie ou les interpolations de caractères par une clé dite clé de Luhn.

Des internautes ont utilisé cette norme et mis, sur leur site Web, un programme capable de générer un vrai-faux numéro de carte à la demande.

L'internaute indélicat peut donc créer, dans une transaction électronique, un vrai-faux numéro de carte, et l'injecter dans une commande sur Internet. Il a peu de chances de tomber sur un numéro réel déjà attribué à un client d'une banque, mais ce risque n'est pas nul car nous avons vu des clients débités par leur banque, lors d'une transaction dont le numéro avait été créé par un site de *carding*, sans que le porteur le sache, sinon à la lecture de son relevé de compte.

A ce stade, il faut rappeler que le risque zéro n'existe pas, y compris dans les moyens de paiement, et on pourrait poursuivre longuement cet inventaire des techniques de fraude. Ces fraudes sont prises très au sérieux par les différents acteurs. Banquiers, commerçants, industriels de la carte et des terminaux, les combattent avec vigueur car elles instillent un comportement anxiogène chez les internautes. En inhibant l'acte d'achat, elles paralysent le développement du commerce électronique. Médiatiquement attractive, la fraude demeure cependant d'une ampleur financière limitée.

Quelques chiffres pour illustrer ce propos :

- le bilan des malversations à l'encontre du système « CB » depuis son origine recense la perte subie par les banques, c'est-à-dire inscrite dans leurs comptes et donc « auditable ». Il n'intègre donc pas les préjudices financiers résultant d'attaques sur les personnes ou sur les biens ;
- la fraude baisse régulièrement depuis 1992 mais, à cause des nouvelles fraudes technologiques, s'accroît légèrement en 1999 et 2000. En 2001, une baisse est attendue, la fraude à la téléphonie mobile ayant été éradiquée par les opérateurs téléphoniques eux-mêmes ;
- elle est et demeure l'un des taux les plus faibles du monde, s'agissant de cartes de débit à utilisation intensive (114 fois par an en moyenne).

En termes de capitaux, les pertes sont très faibles eu égard à l'activité générée par les cartes « CB ». Ainsi, en 2000, sur une

activité évaluée à 1 100 milliards de francs, la fraude au paiement - au sens prédéfini - représente 250 millions de francs, soit 0,023 %, à la charge des banques. A cela, il faut ajouter 70 millions de francs liés à la fraude sur les retraits, soit un total de 320 millions de francs. Il faut, pour comprendre ces chiffres, rappeler par exemple que les chèques sans provision, en 1999, représentaient plus de 15 milliards de francs dont un tiers est resté définitivement à la charge des commerçants.

Ces quelques données démontrent la performance du système de paiement par carte à puce, mais n'excluent pas la question de savoir pourquoi un tel système de paiement est devenu l'une des cibles des *hackers* ?

Le système « CB » repose sur une culture sécuritaire très forte, c'est même ce qui fait son fondement. Le jeu - car c'est d'abord un jeu pour de nombreux *hackers* [2] - consiste à déceler des vulnérabilités et, sous couvert d'un savoir-faire spécifique ou d'une découverte prétendument scientifique, se faire un nom dans le milieu.

Ainsi, casser une clé de 320 bits a plus de retentissement dans le monde des médias que les travaux d'universitaires américains ayant réussi récemment à casser cette même clé, mais d'une longueur double ! Surtout si cet inventeur est condamné par les tribunaux. Il est vrai que les foules se passionnent plus pour Jonathan[3], Mitnick[4], ou Koscher[5], que pour les institutions qui les combattent, et dont elles sont objectivement les victimes.

Une récente évolution, à l'intérieur même du monde des *hackers*, est beaucoup plus préoccupante : le *hacker* ne cherche plus uniquement à trouver une faille pour se faire un nom ; désormais, il veut, le plus souvent, se faire payer. Très concrètement, cela s'appelle extorsion de fonds, chantage ou racket ; car sous couvert officiel de « vendre » sa trouvaille, voire une pseudo-mesure destinée à contrebattre une vulnérabilité mise en évidence, le pirate veut en réalité soutirer illégalement de l'argent de l'institution ou de l'entreprise ainsi attaquée. Le pirate vertueux ou naïf, clamant sa trouvaille pour la beauté du geste, est désormais une image d'Epinal.

A plusieurs reprises, on a pu aussi remarquer que des auxiliaires de justice, sans être les instigateurs directs de cette nouvelle forme de criminalité, n'hésitaient plus à mettre leur savoir, et donc leurs intérêts directs, au service de ces *hackers* dont ils rédigeaient les contrats en prenant soin de prévoir explicitement une clause de versement d'honoraires proportionnelle au chiffre d'affaires « soutiré » à l'issue d'une éventuelle négociation. La déontologie est certainement mise à mal par de telles pratiques, mais est-ce étrange, dès lors que des sommes considérables sont parfois avancées dans ce type de chantage ?

Pour inacceptable qu'il soit, le chantage financier peut être renforcé par des sites Internet dédiés à une affaire. Aux Etats-Unis, ce processus est de pratique courante sous le nom de domaine « *xxsuck.com* ». Dans ce cas, ce site harcèle systématiquement l'entreprise, qui est prise pour cible, utilise les clients déçus, les employés renvoyés et tout autre fait d'actualité pouvant être détourné pour discréditer l'entreprise ou ses dirigeants. Pour marginale que soit cette situation en France à l'heure actuelle, elle se rencontre, et si la loi permet de combattre ces pratiques, il est néanmoins difficile pour une entreprise de contrer ce type d'attaque en raison du poids des médias dans de telles affaires.

Enfin, Internet permettant l'échange et le cumul de savoirs facilite aussi le progrès des connaissances à des fins mafieuses. La mise en facteur commun de parcelles de connaissances sur la carte à puce, l'inconscience extraordinaire de certains professionnels du système qui, pour ne pas paraître incompétents dans un forum, expliquent, détaillent, apportent des solutions aux problèmes successifs auxquels sont confrontés les *hackers*, tout ceci constitue

un autre aspect de la cybercriminalité qu'il faut appréhender. Forums, Chats et sites spécialisés, constituent de formidables réservoirs de déstabilisation où l'on peut, en toute impunité, disséquer un processus pour mieux le ruiner, ou organiser une procédure d'attaque collective sous couvert bien entendu de « recherche »...

On le voit, la cybercriminalité bascule progressivement de son aspect ludique ou technique au chantage et au racket financiers avec l'aide de professionnels. C'est un processus (hélas !) très classique qui est désormais passé du stade de l'expérimentation au rang de pratique courante. Mais, si en définitive le système « CB » n'échappe pas à ce phénomène de cybercriminalité, il conçoit le risque sécuritaire comme un enjeu majeur en ce début de siècle.

À QUEL ENJEU SÉCURITAIRE, LE SYSTEME « CB » DOIT-IL FAIRE FACE ?

Les attaques systématiques ont un seul objectif : déstabiliser un système de paiement en altérant la confiance de ses utilisateurs. Et, plus récemment, cet objectif, avec la Yescard par exemple, est valorisé par l'espoir d'obtenir des biens « gratuitement ». Cette confiance repose sur des mécanismes juridiques eux-mêmes s'appuyant sur une infrastructure technique qui sécurise l'ensemble du dispositif. Et les *hackers* ont bien compris que pour mettre en évidence une vulnérabilité, fût-elle hypothétique, il faut sensibiliser la presse à l'aide de professionnels, et ne pas hésiter à mettre en cause la totalité du système, exigeant tantôt le remplacement immédiat des cartes, tantôt celui des terminaux, voire la nationalisation du système, le tout dans une logorrhée absconse ! Or, il faut se persuader que la technologie de la carte à puce améliore radicalement la confiance dans un système de paiement. En effet, en l'état actuel de la technique, une transaction de paiement se fait classiquement par deux moyens : le système de traitement *on-line* et le système de traitement *off-line*.

Le système de traitement *on-line* est un modèle opératoire d'usage courant dans les pays utilisant des cartes à piste. Dans ce cas, le terminal, après avoir lu la carte, demande à un système central son accord pour effectuer la transaction. Dans la plupart des cas, il n'y a pas de contrôle par un code confidentiel car l'ordre de paiement est juridiquement donné par la signature manuscrite du porteur apposée sur la facturette. Il y a donc deux étapes : une étape d'autorisation électronique, et une étape physique, la signature.

Le système de traitement *off-line* : la technologie de la carte à puce évite, dans la plupart des cas, le recours à une demande d'autorisation sur un serveur parce qu'elle permet, localement par le contrôle du code confidentiel dans la puce, de s'assurer de l'identité du porteur et d'authentifier son consentement par la frappe du code. Dès 1998, la Cour de cassation avait ainsi légitimé le principe de la validité de la signature électronique avant même son incorporation dans notre système juridique par la loi du 13 mars 2000. C'est le modèle utilisé en France depuis 10 ans, et il va vraisemblablement se développer dans le monde entier, puisque Visa et MasterCard ont choisi de migrer à la carte à puce dans les prochaines années.

Enfin, pour être complet, il faut souligner que le système dit *off-line* recourt au serveur d'autorisation selon le montant du paiement. C'est l'une des souplesses offertes par le système « CB » conçu, faut-il le rappeler, à une époque où le coût des demandes d'autorisation par voie téléphonique était prohibitif, et où le système de gestion du risque, mis en place par la technologie de la carte à puce, représentait dans le *business model* une voie alternative prometteuse. Le succès ultérieur des cartes « CB » allait d'ailleurs démontrer l'excel-

lence de cette option économique et la pertinence des choix techniques.

Ainsi, le système « CB » de paiement par carte à puce revêt des aspects de nature juridique différente d'un système d'autorisation en ligne. En effet, dans les systèmes de paiement en ligne, la preuve de la transaction se réalise en deux temps : d'une part, l'intégrité de la piste magnétique est contrôlée lors de la demande d'autorisation (ainsi que d'autres éléments connexes à l'opération en cours), et le terminal du commerçant se borne à recueillir l'accord du serveur bancaire en émettant la facturette. D'autre part, le consentement du porteur est recueilli sur la facturette en y apposant sa signature. Il y a donc un double mécanisme pour matérialiser l'effectivité d'une opération de paiement dans le monde du *on-line* : le numéro d'autorisation et la signature manuscrite.

Pour reconstituer cette chaîne de confiance, à la fois physique et électronique, le système de carte à puce découpe l'opération de paiement en plusieurs phases, dont chacune contribue à établir la confiance que les acteurs doivent légitimement recueillir en utilisant le système. Il faut démontrer :

- l'authenticité de la carte, c'est-à-dire s'assurer que le certificat de celle-ci est reconnu, et qu'il s'inscrit donc bien dans une chaîne hiérarchique de certificats opérant dans le système « CB ». En d'autres termes, il s'agit, pour le système, de vérifier que la carte est reconnue comme acteur valide dans la transaction ;
- l'authentification du porteur : par la frappe du code confidentiel sur le terminal, le porteur « prouve » qu'il est bien le détenteur légitime de cette carte ;
- l'intégrité des données est matérialisée par un sceau (certificat électronique) calculé par la puce à partir des données de la transaction. C'est d'ailleurs ce certificat qui est soumis au serveur pour vérification lorsque le montant requiert une « autorisation » ;
- la non-répudiation du paiement résulte de l'opération effectuée dans ce contexte technique. En effet, celle-ci protège juridiquement le système en rendant opposable au porteur sa propre signature électronique dans l'hypothèse où il la contesterait.

Tout cet ensemble concourt donc à asseoir la preuve lors d'un paiement par carte, et c'est cela le véritable enjeu sécuritaire du système « CB ».

Aussi, les attaques vont-elles se porter sur l'un des trois composants techniques de la transaction pour en ruiner le fondement juridique.

Prenons l'exemple de la Yescard. Cette carte n'est pas une vraie carte, c'est une pseudo-carte « CB », mais elle en revêt tous les aspects.

Concrètement, le pirate s'est introduit par effraction dans le système « CB » et en a modifié les données en recalculant une nouvelle valeur d'authentification à l'aide de la clé RSA 320 bits qui a été cassée. Lorsque la Yescard ainsi modifiée est insérée dans le terminal, ce dernier recalcule la valeur qui lui est présentée et la trouve exacte.

Ensuite, le pirate a altéré (grâce aux différents apports des internautes explicités plus haut) le déroulement initial du dialogue carte/puce en contournant la séquence de vérification du code confidentiel et de calcul du certificat de sorte que, quel que soit le code composé sur le clavier du terminal, la puce répond OK et la transaction se termine par l'édition de la facturette où figure un certificat erroné. Ainsi, le dialogue demeure séquentiellement et techniquement correct, mais sur la base de données fausses.

En résultat de cette transaction, la répudiation est possible puisque le porteur pourra - certificat de la puce édité sur la facturette à l'appui - prouver qu'il n'est pas l'auteur de la transaction contrefaite.

On le voit bien, cette technique est à la fois simple et complexe à mettre en œuvre, mais accessible à des *hackers* ayant le goût

du challenge technique et séduits à l'idée « d'arnaquer » le système bancaire.

Les parades du système « CB » aux attaques des « hackers »

Ce monde serait, en effet, merveilleux pour les *hackers* si le système « CB » n'avait pas anticipé ce type de vulnérabilité et n'avait pas œuvré pour se doter de nouveaux moyens juridiques ou institutionnels pour juguler cette cybercriminalité.

Sur le plan technique, et sans vouloir rentrer dans une explication trop détaillée, le système « CB » a, dès la fin 1999, déployé des cartes à puce avec une clé double, et programmé l'arrivée d'une puce de nouvelle génération de façon à hausser immédiatement le niveau sécuritaire et anticiper de nouvelles évolutions qui verront réellement le jour dans les prochaines années, telles que l'authentification dynamique[6]. Les terminaux seront équipés, fin 2001, notamment dans le commerce de proximité, d'une version unique de traitement de la carte à puce, les dotant du même coup de nouvelles possibilités sophistiquées de lutte contre les fraudes les plus récentes. Ils seront, au même moment, téléparamétrés pour supprimer l'utilisation des clés courtes.

On doit également souligner, dans la panoplie des outils techniques, l'importance de l'effort financier consenti par les banques pour améliorer la sécurité des distributeurs automatiques de billets (DAB). Désormais en France, dans le système « CB », les retraits d'espèces sont effectués en utilisant exclusivement la puce et non la piste[7], supprimant ainsi la fraude par *white plastic* décrite précédemment.

Enfin, une sophistication accrue du traitement des données issues des transactions va modifier substantiellement la qualité de traitement de l'information dans les serveurs bancaires. Ces dispositifs électroniques deviennent ainsi, peu à peu, le nœud gordien de la sécurité du dispositif « CB ».

Au-delà d'un programme sécuritaire très lourd, encadré en outre par la perspective de rejoindre les spécifications internationales EMV et leurs normes sécuritaires, la loi est sur le point d'apporter un certain nombre de réponses positives pour réduire certaines faiblesses juridiques actuelles.

Concrètement, les dispositions législatives prévoient, notamment sous réserve de leur adoption prochaine :
- un cinquième cas d'opposition au paiement permettant désormais au porteur de contester un paiement en cas « d'utilisation frauduleuse de la carte ou des données liées à son utilisation » ;
- une limitation de la responsabilité du porteur à 400 euros pour les transactions qui surviendraient - en cas de perte ou de vol de la carte - avant de faire opposition ;
- une exonération de la responsabilité du porteur lorsque le paiement a été effectué frauduleusement, à distance, sans utilisation physique de sa carte ou lorsque sa carte est contrefaite ou si, « au moment de l'opération contestée, il était en possession physique de sa carte ». Ce dernier cas exonère notamment la responsabilité du porteur en cas d'opérations faites par la technique de *white plastic* évoquée plus haut ;
- un alourdissement significatif des peines : « Est puni de 7 ans d'emprisonnement et de 750 000 euros d'amende, le fait pour toute personne de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition, des équipements, instruments, programmes informatiques ou toutes données, conçus ou spécialement adaptés pour commettre les infractions prévues à l'article L-163-3 §1 et L-163-4 §1 ». Cet article est l'une des dispositions essentielles permettant de lutter efficacement contre les *hackers*, même s'ils ont pris la précaution de déplacer leur site à l'étranger. La justice se montre désormais beaucoup plus ferme à l'égard des *hackers* et contrefacteurs : c'est ainsi que « CB » a

obtenu de poursuivre un site de *carding* établi à l'extérieur de la France et, récemment, un escroc à la carte bancaire vient d'être extradé d'un pays étranger et mis en examen à son arrivée pour « contrefaçon de cartes de paiement et usage » ;
- la loi ordonne également la destruction des instruments contrefaits ou falsifiés et autorise également le juge à prononcer à l'encontre du contrevenant « l'interdiction des droits civiques (…) ainsi que l'interdiction pour une durée de 5 ans ou plus, d'exercer une activité professionnelle ou sociale ».

Enfin, la lutte contre la cybercriminalité repose sur l'action conjointe de la justice et de la police. Il est évident que le procureur de la République dispose d'un rôle prépondérant dans la qualification de l'infraction et dans la mise en œuvre des poursuites en matière de cybercriminalité, d'autant plus que ces incriminations sont nouvelles et parfois complexes à définir. La police, de son côté, est de mieux en mieux outillée pour traquer les *hackers*. Dotée l'an dernier d'un Office central de lutte contre la criminalité liée aux nouvelles technologies de l'information et de la communication, elle vient de se renforcer très récemment en mettant en place une organisation très pointue pour lutter contre le phénomène du piratage dans les cartes à puce.

Ainsi, un remarquable travail de mise à jour des connaissances, de formation et d'information, s'effectue au quotidien pour que policiers, juges et techniciens des cartes, adaptent leurs méthodes et leurs savoirs aux exigences de ces nouvelles technologies qui dépassent très vite nos frontières. Il faut, en effet, souligner l'aspect international que revêt désormais la lutte contre la cybercriminalité, puisqu'un traité devrait être signé prochainement par les membres du Conseil de l'Europe pour faciliter la lutte transfrontière.

La sécurité juridique des opérations par carte se déroule donc dans un cadre dont les objectifs sont clairement définis pour chaque acteur. Les mesures récentes, tant techniques que législatives, visent à renforcer la cohérence du système en organisant mieux, à la fois la protection des droits des consommateurs titulaires d'une carte, mais également les droits des systèmes de carte pour lutter efficacement contre les faussaires car, en définitive, falsifier une carte bancaire, c'est fabriquer de la fausse monnaie.

C'est d'ailleurs l'une des raisons pour lesquelles le législateur a opportunément rappelé le rôle de la Banque de France dans les instruments de paiement, en précisant que celle-ci « s'assure de la sécurité des moyens de paiement… autres que la monnaie fiduciaire ». Il a créé en outre un observatoire de la sécurité des cartes de paiement, de façon à « suivre les mesures de sécurité prises par les émetteurs de carte et proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement ». Ainsi, le législateur a parfaitement intégré que le « phénomène carte » concerne toutes les cartes émises par les banques et les non-banques, car toutes offrent des produits et services exigeant un bon niveau de sécurité pour que les transactions commerciales, qu'elles sous-tendent, se déroulent dans la paix et l'harmonie.

On pourrait légitimement s'étonner de l'intervention récente du législateur dans un système de paiement mis au point et développé par les banques commerciales. Deux remarques viennent spontanément à l'esprit.

D'une part, il s'agit d'un système de paiement devenu véritable phénomène de société, suscitant tour à tour admiration, intérêt, convoitise, voire, le cas échéant, critique ou contestation de la part des utilisateurs qui n'hésitent pas - à bon escient ou non - à questionner la puissance publique, et donc à porter le débat sur les conditions d'utilisation de cet instrument de paiement sur la place publique.

D'autre part, l'Etat, en vertu de sa mission régalienne, est toujours intervenu historiquement pour codifier des initiatives commerciales. Ainsi, le chèque, créé sous le second Empire, a fait l'objet de plusieurs interventions législatives avant d'être codifié dans le décret-loi de 1935, lui-même suivi d'une douzaine de correctifs intervenus au fil des ans pour adapter cet instrument de paiement aux exigences de son temps. La carte bancaire n'échappe pas à cette nécessité, surtout à un moment où la cybercriminalité se développe et attaque directement cet instrument de paiement. C'est en définitive le succès de l'instrument de paiement qui induit l'intervention des pouvoirs publics : personne n'a éprouvé le besoin de réglementer le porte-jeton électronique qui, pour intéressant qu'il soit, est resté à l'état de projet. En revanche, la carte est devenue un phénomène économico-social incontournable, utilisée à plus de 43 millions d'exemplaires pour les cartes « CB », et à plus de 50 millions d'exemplaires pour les autres types de cartes.

La cybercriminalité est un phénomène nouveau, issu des technologies de notre époque. Elle peut tenter de déstabiliser un outil largement répandu dans la société, en tentant d'altérer la confiance des clients. Il appartient donc, à tous les acteurs responsables du bon fonctionnement de cet instrument de paiement et particulièrement aux banques, gestionnaires avisées du risque, de mettre en œuvre, comme elles le font avec vigueur actuellement, les voies et moyens pour réduire ce risque, et poursuivre résolument le développement d'un outil de haute qualité plébiscité par leurs clients.

Notes

1. Précision technique : lorsqu'une carte à puce est insérée dans un terminal, un dialogue de reconnaissance réciproque s'établit par l'intermédiaire d'une série de chiffres appelée valeur d'authentification protégée par un algorithme : la carte fournit la valeur que le terminal vérifie. Si la clé de la valeur d'authentification contenue dans la carte est cassée, le terminal peut être leurré et donne son accord à la poursuite de l'opération.

2. La modélisation de l'attaque contre « CB » par les *hackers* est inspirée des auteurs américains à succès Tom Clancy ou Di Mercurio. Le langage et les codes d'expression sont militaires. Ainsi, la menace actuelle que les *hackers* font peser actuellement sur le système est de niveau « Defcon 2 » c'est-à-dire un niveau d'alerte critique, « Defcon 1 » étant la destruction du système. On reste confondu devant de tels langage et attitude…

3. Jonathan est un jeune pirate suédois de 18 ans en 1999, époque où il a été recruté par le FBI après avoir émis des virus particulièrement sophistiqués sur Internet.

4. Mitnick est un informaticien américain ayant réussi, en 1995, à s'introduire dans les systèmes informatiques de plusieurs grandes entreprises, ayant eu pour effet de jeter la panique.

5. Koscher est également un informaticien qui a mis en évidence, en 1996, une faille dans les puces. Avec un appareillage sophistiqué, il est possible « d'écouter » le différentiel de puissance électrique consommée par la puce lors du calcul du code secret, et de retrouver ce dernier. Cette DPA (*Differential Power Analysis*) est aujourd'hui « traitée » dans les nouvelles puces, notamment par des techniques de compactage.

6. Grâce à cette technologie, à chaque transaction, la valeur d'authentification, au lieu d'être une valeur statique fournie par la carte, est une valeur aléatoire, différente à chaque opération.

7. La piste reste néanmoins présente sur les cartes « CB » pour leur utilisation à l'étranger, où seule la lecture de la piste est possible. De même, les cartes des porteurs étrangers utilisées pour les retraits des espèces sur nos DAB utilisent la piste.